BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

E5569

INFORMATION DELIVERY METHOD AND SYSTEM UTILIZING ZERO INTELLIGENCE PROOF PROTOCOL

Patent Number: JP8149124
Publication date: 1996-06-07
Inventor(s): KANDA MASASUKI; YAMANAKA KIYOSHI; TAKASHIMA YOICHI
Applicant(s):: NIPPON TELEGR & TELEPH CORP <NTT>
Requested Patent: JP8149124
Application Number: JP19950047115 19950307
Priority Number(s):
IPC Classification: H04L9/00 ; H04L9/10 ; H04L9/12 ; G06F13/00 ; G09C1/00
EC Classification:
Equivalents:

Abstract

PURPOSE: To provide an information delivery method and system utilizing the zero intelligence proof protocol by which illegal act is surely prevented by processing simultaneously the process of verifying the user, the process of information delivery and the process of recording and managing communication history data when the user requests the delivery of information to an information server.

CONSTITUTION: A card 1 is used for a random number generating means 12 to generate a random number and sends it to an information server via a communication control means 24. The information server uses a verification means 33 to verify the random number. When the verification is successful, the state is recorded in a history management means 34 as a communication history and managed therein. Then all sets of check texts generated by an information division means 32 are sent. The card 1 links all the sets of the check texts recorded in a storage means 14 and copies an information ciphering secret key and transfer the key to a utility means 23 of the user terminal equipment 2. The utility means 23 decodes the ciphering message stored in the storage means 22 to obtain the message.

E5569

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－149124

(43)公開日　平成８年(1996)６月７日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ 9/00				
9/10				
9/12				
Ｇ０６Ｆ 13/00	３５１	Ｚ 7368－5Ｅ		
			Ｈ０４Ｌ 9/00	Ｚ

審査請求　未請求　請求項の数62　ＯＬ　（全 65 頁）　最終頁に続く

(21)出願番号　特願平7－47115

(22)出願日　平成７年(1995)３月７日

(31)優先権主張番号　特願平6－35797
(32)優先日　平６(1994)３月７日
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平6－213374
(32)優先日　平６(1994)９月７日
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願平6－226282
(32)優先日　平６(1994)９月21日
(33)優先権主張国　日本（ＪＰ）

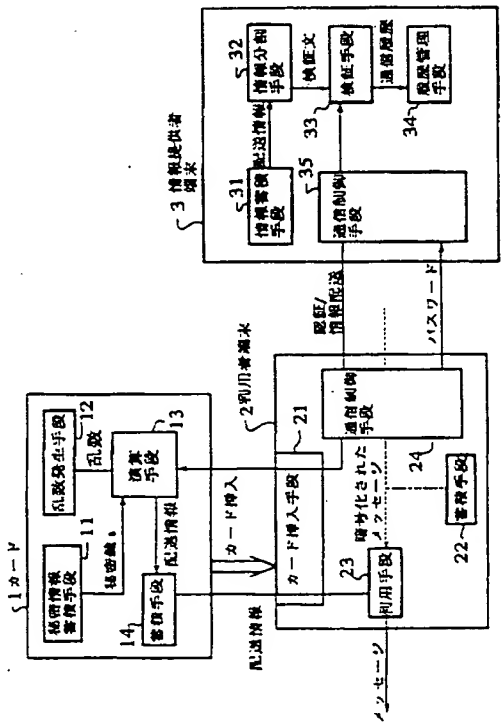
(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号
(72)発明者　神田　雅透
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(72)発明者　山中　喜義
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(72)発明者　高嶋　洋一
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(74)代理人　弁理士　三好　秀和　（外１名）

(54)【発明の名称】　ゼロ知識証明プロトコルを利用した情報配送方法およびシステム

(57)【要約】

【目的】　情報提供者から通信回線により利用者に情報を提供する場合、利用者の正当性と、情報配送の確実性と、配送情報の正当性を保証し、配送情報や受信報告の改竄等の不正行為を防止し、後日これらを証明できる情報配送方法およびシステム。

【構成】　利用者が情報提供者に情報の配送を要求した時に、情報提供者がゼロ知識証明プロトコルにしたがって利用者の利用者認証を行なう過程と、情報提供者が利用者に配送する情報Ｍをゼロ知識証明プロトコル中における検査文Ｅに含めて送信し、利用者に情報を１ビットまたは複数ビット単位で配送する過程と、ゼロ知識証明プロトコルの通信履歴データＨを情報提供者が記録管理する過程と、を同時に行なう。



【特許請求の範囲】
【請求項１】　少なくとも情報提供者と利用者とを含むシステムにおいて、
利用者が情報提供者に情報の配送を要求した時に、
情報提供者が、ゼロ知識証明プロトコルにしたがって利用者の利用者認証を行なう過程と、
情報提供者が、利用者に配送する情報Ｍをゼロ知識証明プロトコル中における検査文Ｅに含めて送信し、利用者に情報を１ビットまたは複数ビット単位で配送する過程と、
情報提供者が、ゼロ知識証明プロトコルの通信履歴データＨを記録管理する過程と、
を同時に行なうことを特徴とする情報配送方法。
【請求項２】　請求項１に記載の情報配送方法において、前記利用者認証を行なう過程及び前記配送する過程は、
利用者が、初期応答文Ｘを情報提供者に送信し、
情報提供者が、利用者に配送する情報Ｍを利用者に送信し、
利用者が、情報Ｍを検査文Ｅとして、初期応答文Ｘと検査文Ｅと利用者の秘密情報Ｓとを用いて応答文Ｙを作成して情報提供者に送信し、
情報提供者が、情報Ｍを検査文Ｅとして、応答文Ｙは初期応答文Ｘと検査文Ｅと利用者の公開情報Ｉとに対する正しい応答になっているかを検査して、利用者の秘密情報Ｓを漏らすことなく、利用者は秘密情報Ｓを知っていることを認証するとともに、利用者は情報Ｍを確実に受信していることを確認することからなる配送確認プロセスを含むことを特徴とする情報配送方法。
【請求項３】　請求項２に記載の情報配送方法において、
情報提供者から利用者に送信する情報Ｍについて暗号通信を行なうことを特徴とする情報配送方法。
【請求項４】　請求項３に記載の情報配送方法において、
利用者から情報提供者に送信する初期応答文Ｘまたは応答文Ｙの少なくともいずれか一方について暗号通信を行なうことを特徴とする情報配送方法。
【請求項５】　請求項１に記載の情報配送方法において、前記利用者認証を行なう過程及び前記配送する過程は、
利用者が、初期応答文Ｘを情報提供者に送信し、
情報提供者が、利用者に配送する情報Ｍを暗号化した暗号文Ｃを利用者に送信し、
利用者が、暗号文Ｃを検査文Ｅとして、初期応答文Ｘと検査文Ｅと利用者の秘密情報Ｓとを用いて応答文Ｙを作成して情報提供者に送信し、
情報提供者が、送信した暗号文Ｃを検査文Ｅとして、応答文Ｙは初期応答文Ｘと検査文Ｅと利用者の公開情報Ｉとに対する正しい応答になっているかを検査して、利用者の秘密情報Ｓを漏らすことなく、利用者は秘密情報Ｓを知っていることを認証するとともに、利用者は暗号文Ｃを確実に受信していることを確認することからなる配送確認プロセスと、
利用者が、暗号文Ｃを復号して情報Ｍを獲得することからなる情報取り出しプロセスとを含むことを特徴とする情報配送方法。
【請求項６】　請求項２から請求項５のいずれかに記載の情報配送方法において、
利用者及び情報提供者は、少なくとも情報Ｍまたは暗号文Ｃを用いて情報圧縮関数により検査文Ｅを作成することを特徴とする情報配送方法。
【請求項７】　請求項２から請求項６のいずれかに記載の情報配送方法において、
利用者及び情報提供者は、少なくとも情報Ｍまたは暗号文Ｃと初期応答文Ｘとを用いて一方向性関数により検査文Ｅを作成することを特徴とする情報配送方法。
【請求項８】　請求項７に記載の情報配送方法において、前記記録管理する過程では、
情報提供者が、少なくとも情報Ｍまたは暗号文Ｃと検査文Ｅと応答文Ｙとからなる通信履歴データＨを記録管理することを特徴とする情報配送方法。
【請求項９】　請求項８に記載の情報配送方法において、更に、
情報提供者が、調停者に対し通信履歴データＨを提示し、
調停者が、検査文Ｅと応答文Ｙと利用者の公開情報Ｉとから初期応答文Ｘを計算し、少なくとも初期応答文Ｘと情報Ｍまたは暗号文Ｃとを用いて一方向性関数により検査文Ｅを作成し、作成した検査文Ｅは通信履歴データＨに含まれる検査文Ｅと一致するかを検査して、一致すれば情報提供者は利用者を認証し、かつ利用者に対して情報Ｍを配送したことを認めることからなる過程を含むことを特徴とする情報配送方法。
【請求項１０】　請求項２から請求項９のいずれかに記載の情報配送方法において、前記利用者認証を行なう過程及び前記配送する過程は、
情報提供者が、利用者に送信する情報Ｍまたは暗号文Ｃを任意ビット長のサイズの複数個のブロックに分割し、各ブロックごとに独立して繰り返し配送確認プロセスを行なうことを特徴とする情報配送方法。
【請求項１１】　請求項１に記載の情報配送方法において、前記利用者認証を行なう過程及び前記配送する過程は、
利用者が、初期応答文Ｘを情報提供者に送信し、
情報提供者が、情報暗号化用秘密鍵Ｗを生成し、利用者に配送する情報Ｍを情報暗号化用秘密鍵Ｗを用いて共通鍵暗号方式により暗号化した暗号文Ｃを利用者に送信し、
利用者が、暗号文Ｃを受信した後、受信した旨を情報提

供者に通知し、
情報提供者が、少なくとも情報暗号化用秘密鍵Ｗを用いて検査文Ｅを生成して利用者に送信し、
利用者が、初期応答文Ｘと検査文Ｅと利用者の秘密情報Ｓとを用いて応答文Ｙを作成して情報提供者に送信し、
情報提供者が、応答文Ｙは初期応答文Ｘと検査文Ｅと利用者の公開情報Ｉとに対する正しい応答になっているかを検査して、利用者の秘密情報Ｓを漏らすことなく、利用者は秘密情報Ｓを知っていることを認証するとともに、利用者は検査文Ｅを確実に受信していることを確認することからなる配送確認プロセスと、
利用者が、少なくとも検査文Ｅを用いて情報暗号化用秘密鍵Ｗを取り出し、情報暗号化用秘密鍵Ｗを用いて共通鍵暗号方式により暗号文Ｃを復号して情報Ｍを獲得することからなる情報取り出しプロセスとを含むことを特徴とする情報配送方法。

【請求項１２】　請求項１１に記載の情報配送方法において、
情報提供者は、少なくとも初期応答文Ｘと乱数文Ｚを用いて一方向性関数により情報暗号化用秘密鍵Ｗを生成することを特徴とする情報配送方法。

【請求項１３】　請求項１２に記載の情報配送方法において、前記記録管理する過程では、
情報提供者が、少なくとも乱数文Ｚと検査文Ｅと応答文Ｙとからなる通信履歴データＨを記録管理することを特徴とする情報配送方法。

【請求項１４】　請求項１３に記載の情報配送方法において、更に、
情報提供者が、調停者に対し通信履歴データＨを提示し、
調停者が、検査文Ｅと応答文Ｙと利用者の公開情報Ｉとから初期応答文Ｘを計算し、少なくとも初期応答文Ｘと乱数文Ｚを用いて一方向性関数により情報暗号化用秘密鍵Ｗを生成し、少なくとも情報暗号化用秘密鍵Ｗを用いて検査文Ｅを作成し、作成した検査文Ｅは通信履歴データＨに含まれる検査文Ｅと一致するかを検査して、一致すれば情報提供者は利用者を認証し、かつ利用者に対して情報Ｍを配送したことを認めることからなる過程とを含むことを特徴とする情報配送方法。

【請求項１５】　請求項１に記載の情報配送方法において、前記利用者認証を行なう過程及び前記配送する過程は、
情報提供者が、情報暗号化用秘密鍵Ｗを生成し、情報Ｍを情報暗号化用秘密鍵Ｗを用いて共通鍵暗号方式により暗号化した暗号文Ｃを利用者に送信し、
利用者が、暗号文Ｃを受信した後、受信した旨を情報提供者に通知することからなる情報配送プロセスと、
利用者が、初期応答文Ｘを情報提供者に送信し、
情報提供者が、少なくとも情報暗号化秘密鍵Ｗを用いて検査文Ｅを作成して利用者に送信し、
利用者が、初期応答文Ｘと検査文Ｅと利用者の秘密情報Ｓとを用いて応答文Ｙを作成して情報提供者に送信し、
情報提供者が、応答文Ｙは初期応答文Ｘと検査文Ｅと利用者の公開情報Ｉとに対する正しい応答になっているかを検査して、利用者の秘密情報Ｓを漏らすことなく、利用者は秘密情報Ｓを知っていることを認証するとともに、利用者は検査文Ｅを確実に受信していることを確認することからなる配送確認プロセスと、
利用者が、少なくとも検査文Ｅを用いて情報暗号化用秘密鍵Ｗを獲得し、情報暗号化用秘密鍵Ｗを用いて共通鍵暗号方式により暗号文Ｃを復号して情報Ｍを獲得することからなる情報取り出しプロセスとを含むことを特徴とする情報配送方法。

【請求項１６】　請求項１５に記載の情報配送方法において、
情報提供者は少なくとも自ら生成した乱数文Ｚを用いて一方向性関数により情報暗号化用秘密鍵Ｗを生成することを特徴とする情報配送方法。

【請求項１７】　請求項１６に記載の情報配送方法において、
前記配送確認プロセスでは、情報提供者は少なくとも初期応答文Ｘを用いて一方向性関数により鍵暗号化用秘密鍵Ｋを生成し、少なくとも情報暗号化用秘密鍵Ｗと鍵暗号化用秘密鍵Ｋとを用いて検査文Ｅを生成して利用者に送信し、
前記情報取り出しプロセスでは、利用者は少なくとも初期応答文Ｘを用いて一方向性関数により鍵暗号化用秘密鍵Ｋを生成し、少なくとも検査文Ｅと鍵暗号化用秘密鍵Ｋとを用いて情報暗号化用秘密鍵Ｗを取り出すことを特徴とする情報配送方法。

【請求項１８】　請求項１７に記載の情報配送方法において、前記記録管理する過程では、
情報提供者が、少なくとも乱数文Ｚと検査文Ｅと応答文Ｙとからなる通信履歴データＨを記録管理することを特徴とする情報配送方法。

【請求項１９】　請求項１８に記載の情報配送方法において、更に、
情報提供者が調停者に対し通信履歴データＨを提示し、
調停者が検査文Ｅと応答文Ｙと利用者の公開情報Ｉとから初期応答文Ｘを計算し、少なくとも初期応答文Ｘを用いて一方向性関数により鍵暗号用秘密鍵Ｋを、また少なくとも乱数文Ｚを用いて一方向性関数により情報暗号化用秘密鍵Ｗをそれぞれ生成し、少なくとも鍵暗号用秘密鍵Ｋと情報暗号化用秘密鍵Ｗとを用いて検査文Ｅを作成し、作成した検査文Ｅは通信履歴データＨに含まれる検査文Ｅと一致するかを検査して、一致すれば情報提供者は利用者を認証し、かつ利用者に対して情報Ｍを配送したことを認めることからなる過程を含むことを特徴とする情報配送方法。

【請求項２０】　請求項１６に記載の情報配送方法にお

いて、
前記配送確認プロセスでは、情報提供者は少なくとも初期応答文Ｘおよび利用者と情報提供者が秘密に共有している秘密情報ＣＳとを用いて一方向性関数により鍵暗号化用秘密鍵Ｋを生成し、少なくとも情報暗号化用秘密鍵Ｗと鍵暗号化用秘密鍵Ｋとを用いて検査文Ｅを生成して利用者に送信し、
前記情報取り出しプロセスでは、利用者は少なくとも初期応答文Ｘと秘密情報ＣＳとを用いて一方向性関数により鍵暗号化用秘密鍵Ｋを生成し、少なくとも検査文Ｅと鍵暗号化用秘密鍵Ｋとを用いて情報暗号化用秘密鍵Ｗを取り出すことを特徴とする情報配送方法。
【請求項２１】　請求項２０に記載の情報配送方法において、前記記録管理する過程では、
情報提供者が、少なくとも利用者と情報提供者が秘密に共有している秘密情報ＣＳと乱数文Ｚと検査文Ｅと応答文Ｙとからなる通信履歴データＨを記録管理することを特徴とする情報配送方法。
【請求項２２】　請求項２１に記載の情報配送方法において、更に、
情報提供者が調停者に対し通信履歴データＨを提示し、
調停者が検査文Ｅと応答文Ｙと利用者の公開情報Ｉとから初期応答文Ｘを計算し、少なくとも初期応答文Ｘおよび利用者と情報提供者が秘密に共有している秘密情報ＣＳとを用いて一方向性関数により鍵暗号用秘密鍵Ｋを、また少なくとも乱数文Ｚを用いて一方向性関数により情報暗号化用秘密鍵Ｗをそれぞれ生成し、少なくとも鍵暗号用秘密鍵Ｋと情報暗号化用秘密鍵Ｗとを用いて検査文Ｅを作成し、作成した検査文Ｅは通信履歴データＨに含まれる検査文Ｅと一致するかを検査して、一致すれば情報提供者は利用者を認証し、かつ利用者に対して情報Ｍを配送したことを認めることから成る過程を含むことを特徴とする情報配送方法。
【請求項２３】　請求項１５に記載の情報配送方法において、
利用者は、要求文Ｒを情報提供者に送信し、
情報提供者は、少なくとも要求文Ｒと自ら生成した乱数文Ｚとを用いて一方向性関数により情報暗号化用秘密鍵Ｗを生成することを特徴とする情報配送方法。
【請求項２４】　請求項２３に記載の情報配送方法において、
利用者から情報提供者に送信する要求文Ｒについて暗号通信を行なうことを特徴とする情報配送方法。
【請求項２５】　請求項２３または請求項２４に記載の情報配送方法において、
前記配送確認プロセスでは、情報提供者が、少なくとも初期応答文Ｘを用いて一方向性関数により鍵暗号化用秘密鍵Ｋを生成し、少なくとも情報暗号化用秘密鍵Ｗと鍵暗号化用秘密鍵Ｋとを用いて検査文Ｅを生成して利用者に送信し、
前記情報取り出しプロセスでは、利用者が、少なくとも初期応答文Ｘを用いて一方向性関数により鍵暗号化用秘密鍵Ｋを生成し、少なくとも検査文Ｅと鍵暗号化用秘密鍵Ｋとを用いて情報暗号化用秘密鍵Ｗを取り出すことを特徴とする情報配送方法。
【請求項２６】　請求項２５に記載の情報配送方法において、前記記録管理する過程では、
情報提供者が、少なくとも乱数文Ｚと検査文Ｅと応答文Ｙと要求文Ｒとからなる通信履歴データＨを記録管理することを特徴とする情報配送方法。
【請求項２７】　請求項２６に記載の情報配送方法において、更に、
情報提供者が、調停者に対し通信履歴データＨを提示し、
調停者が、検査文Ｅと応答文Ｙと利用者の公開情報Ｉとから初期応答文Ｘを計算し、少なくとも初期応答文Ｘを用いて一方向性関数により鍵暗号用秘密鍵Ｋを、また少なくとも乱数文Ｚと要求文Ｒとを用いて一方向性関数により情報暗号化用秘密鍵Ｗをそれぞれ生成し、少なくとも鍵暗号用秘密鍵Ｋと情報暗号化用秘密鍵Ｗとを用いて検査文Ｅを作成し、作成した検査文Ｅは通信履歴データＨに含まれる検査文Ｅと一致するかを検査して、一致すれば情報提供者は利用者を認証し、かつ利用者に対して情報Ｍを配送したことを認めることからなる過程を含むことを特徴とする情報配送方法。
【請求項２８】　請求項２３または請求項２４に記載の情報配送方法において、
前記配送確認プロセスでは、情報提供者が、少なくとも初期応答文Ｘおよび利用者と情報提供者が秘密に共有している秘密情報ＣＳとを用いて一方向性関数により鍵暗号化用秘密鍵Ｋを生成し、少なくとも情報暗号化用秘密鍵Ｗと鍵暗号化用秘密鍵Ｋとを用いて検査文Ｅを生成して利用者に送信し、
前記情報取り出しプロセスでは、利用者が、少なくとも初期応答文Ｘと秘密情報ＣＳとを用いて一方向性関数により鍵暗号化用秘密鍵Ｋを生成し、少なくとも検査文Ｅと鍵暗号化用秘密鍵Ｋとを用いて情報暗号化用秘密鍵Ｗを取り出すことを特徴とする情報配送方法。
【請求項２９】　請求項２８に記載の情報配送方法において、前記記録管理する過程では、
情報提供者が、少なくとも利用者と情報提供者が秘密に共有している秘密情報ＣＳと乱数文Ｚと検査文Ｅと応答文Ｙと要求文Ｒとからなる通信履歴データＨを記録管理することを特徴とする情報配送方法。
【請求項３０】　請求項２９に記載の情報配送方法において、更に、
情報提供者が、調停者に対し通信履歴データＨを提示し、
調停者が、検査文Ｅと応答文Ｙと利用者の公開情報Ｉとから初期応答文Ｘを計算し、少なくとも初期応答文Ｘお

よび利用者と情報提供者が秘密に共有している秘密情報ＣＳとを用いて一方向性関数により鍵暗号用秘密鍵Ｋを、また少なくとも乱数文Ｚと要求文Ｒとを用いて一方向性関数により情報暗号化用秘密鍵Ｗをそれぞれ生成し、少なくとも鍵暗号用秘密鍵Ｋと情報暗号化用秘密鍵Ｗとを用いて検査文Ｅを作成し、作成した検査文Ｅは通信履歴データＨに含まれる検査文Ｅと一致するかを検査して、一致すれば情報提供者は利用者を認証し、かつ利用者に対して情報Ｍを配送したことを認めることから成る過程を含むことを特徴とする情報配送方法。

【請求項３１】　請求項１５に記載の情報配送方法において、更に、

情報提供者が、利用者には復号できない方式で暗号化した情報暗号化用秘密鍵ＣＷを利用者に送信し、

利用者が、暗号化された情報暗号化用秘密鍵ＣＷにディジタル署名した署名付き情報暗号用秘密鍵ＳＷを情報提供者に送信し、

情報提供者が、署名付き情報暗号用秘密鍵ＳＷの署名は正しいかを検証することからなる過程を含むことを特徴とする情報配送方法。

【請求項３２】　請求項３１に記載の情報配送方法において、

前記配送確認プロセスでは、情報提供者が、少なくとも初期応答文Ｘを用いて一方向性関数により鍵暗号化用秘密鍵Ｋを生成し、少なくとも情報暗号化用秘密鍵Ｗと鍵暗号化用秘密鍵Ｋとを用いて検査文Ｅを生成して利用者に送信し、

前記情報取り出しプロセスでは、利用者が、少なくとも初期応答文Ｘを用いて一方向性関数により鍵暗号化用秘密鍵Ｋを生成し、少なくとも検査文Ｅと鍵暗号化用秘密鍵Ｋとを用いて情報暗号化用秘密鍵Ｗを取り出すことを特徴とする情報配送方法。

【請求項３３】　請求項３２に記載の情報配送方法において、前記記録管理する過程では、

情報提供者が、少なくとも情報暗号用秘密鍵Ｗと署名付き情報暗号用秘密鍵ＳＷと検査文Ｅと応答文Ｙとからなる通信履歴データＨを記録管理することを特徴とする情報配送方法。

【請求項３４】　請求項３３に記載の情報配送方法において、更に、

情報提供者が、調停者に対し通信履歴データＨを提示し、

調停者が、署名付き情報暗号用秘密鍵ＳＷは情報暗号用秘密鍵Ｗに対する正しい署名であるかどうかを検証した後、検査文Ｅと応答文Ｙと利用者の公開情報Ｉとから初期応答文Ｘを計算し、少なくとも初期応答文Ｘを用いて一方向性関数により鍵暗号用秘密鍵Ｋを生成し、少なくとも鍵暗号用秘密鍵Ｋと情報暗号化用秘密鍵Ｗとを用いて検査文Ｅを作成し、作成した検査文Ｅは通信履歴データＨに含まれる検査文Ｅと一致するかを検査して、一致すれば情報提供者は利用者を認証し、かつ利用者に対して情報Ｍを配送したことを認めることからなる過程を含むことを特徴とする情報配送方法。

【請求項３５】　請求項３１に記載の情報配送方法において、

前記配送確認プロセスでは、情報提供者は少なくとも初期応答文Ｘ及び利用者と情報提供者が秘密に共有している秘密情報ＣＳを用いて一方向性関数により鍵暗号化用秘密鍵Ｋを生成し、少なくとも情報暗号化用秘密鍵Ｗと鍵暗号化用秘密鍵Ｋとを用いて検査文Ｅを生成して利用者に送信し、

前記情報取り出しプロセスでは、利用者は少なくとも初期応答文Ｘ及び利用者と情報提供者が秘密に共有している秘密情報ＣＳを用いて一方向性関数により鍵暗号化用秘密鍵Ｋを生成し、少なくとも検査文Ｅと鍵暗号化用秘密鍵Ｋとを用いて情報暗号化用秘密鍵Ｗを取り出すことを特徴とする情報配送方法。

【請求項３６】　請求項３５に記載の情報配送方法において、前記記録管理する過程では、

情報提供者が、少なくとも情報暗号用秘密鍵Ｗと署名付き情報暗号用秘密鍵ＳＷと検査文Ｅと応答文Ｙ及び利用者と情報提供者が秘密に共有している秘密情報ＣＳとからなる通信履歴データＨを記録管理することを特徴とする情報配送方法。

【請求項３７】　請求項３６に記載の情報配送方法において、更に、

情報提供者が調停者に対し通信履歴データＨを提示し、

調停者が署名付き情報暗号用秘密鍵ＳＷは情報暗号用秘密鍵Ｗに対する正しい署名であるかどうかを検証した後、検査文Ｅと応答文Ｙと利用者の公開情報Ｉとから初期応答文Ｘを計算し、少なくとも初期応答文Ｘ及び利用者と情報提供者が秘密に共有している秘密情報ＣＳを用いて一方向性関数により鍵暗号用秘密鍵Ｋを生成し、少なくとも鍵暗号用秘密鍵Ｋと情報暗号化用秘密鍵Ｗとを用いて検査文Ｅを作成し、作成した検査文Ｅは通信履歴データＨに含まれる検査文Ｅと一致するかを検査して、一致すれば情報提供者は利用者を認証し、かつ利用者に対して情報Ｍを配送したことを認めることからなる過程を含むことを特徴とする情報配送方法。

【請求項３８】　請求項１１から請求項３７のいずれかに記載の情報配送方法において、

情報提供者から利用者に送信する検査文Ｅについて暗号通信を行なうことを特徴とする情報配送方法。

【請求項３９】　請求項３８の情報配送方法において、利用者から情報提供者に送信する初期応答文Ｘまたは応答文Ｙの少なくとも一方を暗号通信を行なうことを特徴とする情報配送方法。

【請求項４０】　請求項１１から請求項３７のいずれかに記載の情報配送方法において、

前記配送確認プロセスでは、情報提供者が、少なくとも

検査文Ｅを暗号化して利用者に送信し、
前記情報取り出しプロセスでは、利用者が、検査文Ｅを復号することを特徴とする情報配送方法。
【請求項４１】　請求項１１から請求項４０のいずれかに記載の情報配送方法において、前記利用者認証を行なう過程及び前記配送する過程は、
検査文Ｅを任意ビット長のサイズの複数個のブロックに分割し、各ブロックごとに独立して繰り返し配送確認プロセスを行なうことを特徴とする情報配送方法。
【請求項４２】　請求項１から請求項４１のいずれかに記載の情報配送方法において、
利用者側の動作は携帯可能な利用者のカードによって実行されることを特徴とする情報配送方法。
【請求項４３】　請求項１から請求項４２のいずれかに記載の情報配送方法において、更に、
前記形態可能な利用者のカードに利用者が受信した情報Ｍまたは情報暗号用秘密鍵Ｗを記録することを含むことを特徴とする情報配送方法。
【請求項４４】　少なくとも利用者端末と情報提供者端末とを含むシステムであって、
利用者端末は、
情報提供者端末との間の通信を制御する利用者通信制御手段と、
利用者が秘密に保持すべき秘密情報を蓄積しておく利用者秘密情報蓄積手段と、
乱数を発生する乱数発生手段と、
前記利用者通信制御手段を介して通信される初期応答文と応答文を前記秘密情報と乱数に基づいて生成する利用者演算手段とを有し、
情報提供者端末は、
利用者端末との間の通信を制御する情報提供者通信制御手段と、
前記情報提供者通信制御手段を介して利用者に提供する情報を蓄積しておく情報データベースと、
前記情報提供者通信制御手段を介して利用者の認証を行なう検証手段とを有することを特徴とする情報配送システム。
【請求項４５】　請求項４４に記載の情報配送システムにおいて、
利用者端末は更に前記利用者通信制御手段を介して情報提供者から配送された情報を蓄積する情報蓄積手段を有することを特徴とする情報配送システム。
【請求項４６】　請求項４４または請求項４５に記載の情報配送システムにおいて、
利用者端末および情報提供者端末の双方が更に共通鍵暗号方式または公開鍵暗号方式、もしくはその両方の暗号方式による暗号通信を行う暗号手段を有することを特徴とする情報配送システム。
【請求項４７】　請求項４６に記載の情報配送システムにおいて、
情報提供者端末は更に前記暗号手段で利用される情報提供者が秘密に保持すべき情報を蓄積する情報提供者秘密情報蓄積手段を有することを特徴とする情報配送システム。
【請求項４８】　請求項４４から請求項４７のいずれかに記載の情報配送システムにおいて、
利用者端末の前記利用者演算手段および情報提供者端末の前記検証手段の双方が情報圧縮関数または一方向性関数、もしくはその両方の関数による関数演算を行う手段を有することを特徴とする情報配送システム。
【請求項４９】　請求項４４から請求項４８のいずれかに記載の情報配送システムにおいて、
情報提供者端末は更に通信履歴データを記録管理する通信履歴ファイルを有することを特徴とする情報配送システム。
【請求項５０】　請求項４９に記載の情報配送システムにおいて、更に、
情報提供者が利用者に情報を提供したことを照明する通信履歴データについて、通信履歴データの正当性を検査する調停端末であって、
初期応答文と検査文を生成する調停演算手段と、
通信履歴データ中の検査文と前記調停演算手段で生成した検査文とに基づいて該通信履歴データの正当性を検査する調停検証手段とを有するものを含むことを特徴とする情報配送システム。
【請求項５１】　請求項４４から請求項５０のいずれかに記載の情報配送システムにおいて、
情報提供者端末は更に前記情報提供者通信制御手段を介して利用者へ配送する情報を任意ビット長サイズの複数のブロックに分割する情報分割手段を有し、
利用者端末は更に前記複数個のブロックに分割された情報を元の情報に再構成する情報再構成手段を有することを特徴とする情報配送システム。
【請求項５２】　少なくとも利用者端末と情報提供者端末とを含むシステムであって、
利用者端末は、
情報提供者端末との間の通信を制御する利用者通信制御手段と、
利用者が秘密に保持すべき秘密情報を蓄積しておく利用者秘密情報蓄積手段と、
前記利用者通信制御手段を介して情報提供者端末との間で暗号通信を行う利用者共通鍵暗号手段と、
乱数を発生する乱数発生手段と、
前記利用者通信制御手段を介して通信される初期応答文と応答文と秘密鍵を生成する利用者演算手段と、
前記利用者通信制御手段を介して情報提供者から配送された情報を蓄積する情報蓄積手段とを有し、
情報提供者端末は、
利用者端末との間の通信を制御する情報提供者通信制御手段と、

前記情報提供者通信制御手段を介して利用者に提供する情報を蓄積しておく情報データベースと、
秘密鍵と検査文を生成する情報提供者演算手段と、
前記情報提供者通信制御手段を介して利用者端末との間で暗号通信を行う情報提供者共通鍵暗号手段と、
前記情報提供者通信制御手段を介して利用者の認証を行なう検証手段とを有することを特徴とする情報配送システム。

【請求項５３】　請求項５２に記載の情報配送システムにおいて、
情報提供者端末は更に前記情報提供者演算手段で利用される乱数を発生する乱数発生手段を有することを特徴とする情報配送システム。

【請求項５４】　請求項５２または請求項５３に記載の情報配送システムにおいて、
利用者端末および情報提供者端末の双方が更に公開鍵暗号方式による暗号通信を行なう公開鍵暗号手段をを有することを特徴とする情報配送システム。

【請求項５５】　請求項５２から請求項５４のいずれかに記載の情報配送システムにおいて、
情報提供者端末は更に前記情報提供者演算手段または前記公開鍵暗号手段で利用される情報提供者が秘密に保持すべき情報を蓄積する情報提供者秘密情報蓄積手段を有することを特徴とする情報配送システム。

【請求項５６】　請求項５２から請求項５５のいずれかに記載の情報配送システムにおいて、
利用者端末は更にディジタル署名を行うディジタル署名手段を有し、
情報提供者端末はディジタル署名を検証するためのディジタル署名検証手段を有することを特徴とする情報配送システム。

【請求項５７】　請求項５２から請求項５６のいずれかに記載の情報配送システムにおいて、
情報提供者端末は更に通信履歴データを記録管理する通信履歴ファイルを有することを特徴とする情報配送システム。

【請求項５８】　請求項５７に記載の情報配送システムにおいて、更に、
情報提供者が利用者に情報を提供したことを証明する通信履歴データについて、通信履歴データの正当性を検査する調停端末であって、
初期応答文と秘密鍵と検査文を生成する調停演算手段と、
通信履歴データ中の検査文と前記調停演算手段で生成した検査文とに基づいて該通信履歴データの正当性を検査する調停検証手段とを有するものを含むことを特徴とする情報配送システム。

【請求項５９】　請求項５８に記載の情報配送システムにおいて、
調停端末が更に通信履歴データ中の署名付き情報暗号用秘密鍵の署名は正当であるかを検証する検証手段を有することを特徴とする情報配送システム。

【請求項６０】　請求項５２から請求項５９のいずれかに記載の情報配送システムにおいて、
情報提供者端末は更に前記情報提供者通信制御手段を介して利用者へ配送する情報を任意ビット長サイズの複数のブロックに分割する情報分割手段を有し、
利用者端末は更に前記複数個のブロックに分割された情報を元の情報に再構成する情報再構成手段を有することを特徴とする情報配送システム。

【請求項６１】　請求項４４から請求項６０のいずれかに記載の情報配送システムにおいて、
利用者端末は前記利用者秘密鍵蓄積手段、乱数発生手段、利用者演算手段を含んだカードと、
該カードが挿入されるカード挿入手段とを有することを特徴とする情報配送システム。

【請求項６２】　請求項６１に記載の情報配送システムにおいて、
前記カードは更に情報提供者から配送された情報を蓄積する情報カード蓄積手段を有することを特徴とする情報配送システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、電気通信システムを用いて利用者が要求した情報を情報提供者が提供する場合に、情報提供者が利用者認証により利用者の正当性を認証しつつ、かつ利用者に要求された情報を利用者まで確実に配送するとともに、後日利用者から要求した情報を受信していないなどの異議申し立てに対して、情報提供者が間違いなく要求された情報を利用者に配送し、かつ利用者が受信している事実を証明できるようにするためのものであり、特に有料情報提供サービスや配達証明サービスなどに有用な情報配送方法およびシステムに関する。

【０００２】

【従来の技術】従来、代表的な認証方法としてはシステム利用者の正当性を検査する利用者認証方式と、情報が正当なものであることを証明するメッセージ認証方式と、更にこれらを組み合わせて作成した情報が正当なものであることを情報作成者が保証するディジタル署名方式がある。ここで、簡単に利用者認証方式とメッセージ認証方式とディジタル署名方式について、それぞれ図を参照しながら説明する。

【０００３】図１（ａ）は利用者認証方式の代表的な例であるFiat Shamir 法（A.Fiat andA.Shamir: "How to prove yourself,practical solutions to identificationand signature problems", Proc. of Crypto' 86,1986.5並びに米国特許第4,748,668 号）による認証方式の概念図である。

【０００４】このFiat Shamir 法によれば、秘密情報s

を所有している者（以下、証明者という）が検証者に対してその正当性を証明しようとしたとき、Ｎ（＝ｐｑ：ｐ，ｑは互いに異なる大きな素数）とＩ（＝s^2（mod Ｎ））を証明者の公開情報とし、ｓとｐ，ｑを証明者の秘密情報として以下のように認証される。

【０００５】まず始めに証明者が乱数Ｒを生成させ、初期応答文Ｘ＝R^2（mod Ｎ）を計算し、検証者にＸを送る。前記Ｘを受信した検証者は検査文ｅとしてランダムに０または１を選び、証明者にｅを送る。前記ｅを受信した証明者は、応答文Ｙ＝Ｒs^e（mod Ｎ）を計算し、検証者にＹを送る。前記Ｙを受信した検証者は、検証式Y^2＝Ｘ×I^e（mod Ｎ）が成立するかを検証する。

【０００６】ここまでを１ラウンドとして、これをｔラウンド繰り返すことにより、秘密情報ｓを知らない第三者が検証者の検証式をクリアできる確率は（１／2^t）となる。したがって、十分に大きなｔにおいて正常に認証が終了した場合、検証者は検証相手（証明者）を秘密情報ｓを所有している正当な証明者であると判断して構わない。

【０００７】なお、この認証方式は一般にゼロ知識証明に基づく認証方式と呼ばれ、証明者は検証者に対して秘密情報ｓを所有している事実だけを伝え、秘密情報ｓに関するその他の内容は一切漏らさないというメリットがある。

【０００８】しかし、Fiat Shamir 法では証明者と検証者との通信履歴が、後日検証者が証明者を認証したことの証拠にならないという問題があった。そのため、この問題に対する解決方法としては桜井（特開平５－１２３２１号）による認証方式が提案されている。この認証方式によれば、検証者が証明者を認証した後でも検証者が証明者を本当に認証したことの証拠が残るとされている。

【０００９】しかし、ここで証拠として残るのはあくまで検証者が証明者を通信を介して認証したという事実についてのみであり、この認証事実の他は通信内容を始めとしてどのような通信が行われたのかについて何ら言及するものではない。また、認証事実の証拠として通信系列全てを記録保管するため、検証者が記録保管しておかなければならない情報量が多いという欠点もある。

【００１０】次に、図１（ｂ）は、メッセージ認証の一例である認証子法による認証方式の概念図である。この認証方式によれば、メッセージＭを送信したい証明者は秘密鍵K_hをパラメータとするハッシュ関数ｈを利用してメッセージＭに対する認証子h_k（Ｍ）を作成し、前記メッセージＭと共に前記認証子を送信相手である検証者に送信する。検証者はあらかじめ証明者と同じ秘密鍵K_hを秘密裏に共有しているので、受信したメッセージから上記と同じように秘密鍵K_hを用いて認証子を作成し、受信した認証子と照合検査する。この照合に成功すれば、受信したメッセージの正当性が保証される。これは秘密鍵K_hを知らなければ、任意のメッセージに対する正しい認証子は作成できないためである。

【００１１】しかし、上記の利用者認証、メッセージ認証は共に、基本的には第三者による不正行為を防止することが最大の目的であり、前記利用者認証が正常に終了したことで保証されるのは、あくまで証明者が正当な秘密情報の所有者であること、すなわち第三者が不正に利用していないということだけであり、また前記メッセージ認証において照合検査に成功したことで保証されるのは、第三者によるメッセージの改竄などの不正行為が行われていないということだけである。したがって、上記の２つの認証方式は共に、基本的には第三者の不正行為に対してのみ有効であり、証明者もしくは検証者による不正行為に対してはまるで効力を持たないのが欠点である。

【００１２】次に、図１（ｃ）はディジタル署名の一例であるＲＳＡ署名法（R.L.Rivest, A.Shamir, L.Adleman, “A method for obtaining digital signatures and public-key cryptosystem”, Comm. ACM, vol.21, No.2, 1978.2）の概念図である。

【００１３】ＲＳＡ署名法によれば、ｅとＮ（＝ｐｑ：ｐ，ｑは互いに異なる大きな素数）を署名者の公開情報、ｄ［ｅ×ｄ（mod(p-1)(q-1))＝１］とｐ，ｑを署名者の秘密情報として以下のように認証される。

【００１４】まず署名者は、メッセージＭを確かに署名者が作成したものであることを保証するために署名文Ｃ＝M^d（mod Ｎ）を計算し、Ｃを検証者に送信する。前記Ｃを受信した検証者はＭ＝C^e（mod Ｎ）を計算し、得られたメッセージＭの正当性を判断する。この時、得られたメッセージＭが正当であると判断されれば、受信したメッセージＭが署名者により間違いなく作成されたものであることが保証される。

【００１５】これは秘密情報ｄを知らなければ任意のメッセージに対する正しい署名文を作成できないためであり、しかも秘密情報ｄは各個人固有のもので一人ずつ異なるため、署名者自体も特定されることになるからである。したがって、第三者や検証者がメッセージ内容を改竄したり、あるいは署名者がメッセージ内容を否定したりするなどの不正行為は困難であると考えられている。

【００１６】しかし、これはあくまでメッセージのやり取りが正常に終了した時点以後から効力が生じるものであり、それ以前、すなわち署名者からみて送信した署名文Ｃが確実に検証者に届いているかどうかの保証は何もないため、検証者に署名文Ｃを受信していないと主張されてしまえば、署名者にはその主張に対抗する手段がないのが欠点である。

【００１７】

【発明が解決しようとする課題】利用者が要求した情報を情報提供者が提供する場合には以下の４条件、すなわち、（１）正当な利用者であることを保証する利用者認

証、（２）情報提供者は利用者が要求した情報を確実に提供し、かつ利用者が提供された情報を受信したことを保証する配送証明、（３）提供した情報が正当なものであり、改竄などの不正行為を防止できる内容照明、（４）後日、必要に応じて情報提供者が調停者に通信履歴などの証拠を提示することにより（１）～（３）のすべてについて証明できること、を満たすことが必要である。

【００１８】しかし、従来方式で説明したようにFiat Shamir 法では（１）のみ、桜井（特開平５－１２３２１号）の方式では（１）と（４）の一部（利用者認証の証拠のみ）、メッセージ証拠では（３）の一部のみ（情報が正当である保証のみ）、ＲＳＡ署名法では（３）のみが満たされるだけであるため、ある種の不正行為、特に（２）のように利用者が提供された情報を受信しているにもかかわらず、受信していないというような不当な主張に対して、情報提供者は全く対抗できないという欠点がある。

【００１９】本発明の目的は、情報提供者から利用者（カード、利用者端末等を含む）に対して必要なメッセージを送信する場合に、従来方式では満たせなかった上記の４条件すべてを満たすことができるゼロ知識証明プロトコルを利用した情報配送方法およびシステムを提供することである。

【００２０】

【課題を解決するための手段】本発明の一側面によると、少なくとも情報提供者と利用者とを含むシステムにおいて、利用者が情報提供者に情報の配送を要求した時に、情報提供者が、ゼロ知識証明プロトコルにしたがって利用者の利用者認証を行なう過程と、情報提供者が利用者に配送する情報Ｍをゼロ知識証明プロトコル中における検査文Ｅに含めて送信し、利用者に情報を１ビットまたは複数ビット単位で配送する過程と、情報提供者が、ゼロ知識証明プロトコルの通信履歴データＨを記録管理する過程とを同時に行なうことを特徴とする情報配送方法が提供される。

【００２１】また、本発明の他の側面によると、少なくとも利用者端末と情報提供者端末とを含むシステムであって、利用者端末は、情報提供者端末との間の通信を制御する利用者通信制御手段と、利用者が秘密に保持すべき秘密情報を蓄積しておく利用者秘密情報蓄積手段と、乱数を発生する乱数発生手段と、前記利用者通信制御手段を介して通信される初期応答文と応答文を前記秘密情報と乱数に基づいて生成する利用者演算手段とを有し、情報提供者端末は、利用者端末との間の通信を制御する情報提供者通信制御手段と、前記情報提供者通信制御手段を介して利用者に提供する情報を蓄積しておく情報データベースと、前記情報提供者通信制御手段を介して利用者の認証を行なう検証手段とを有することを特徴とする情報配送システムが提供される。

【００２２】また、本発明の他の側面によると、少なくとも利用者端末と情報提供者端末とを含むシステムであって、利用者端末は、情報提供者端末との間の通信を制御する利用者通信制御手段と、利用者が秘密に保持すべき秘密情報を蓄積しておく利用者秘密情報蓄積手段と、前記利用者通信制御手段を介して情報提供者端末との間で暗号通信を行う利用者共通鍵暗号手段と、乱数を発生する乱数発生手段と、前記利用者通信制御手段を介して送信される初期応答文と応答文と秘密鍵を生成する利用者演算手段と、前記利用者通信制御手段を介して情報提供者から配送された情報を蓄積する情報蓄積手段とを有し、情報提供者端末は、利用者端末との間の通信を制御する情報提供者通信制御手段と、前記情報提供者通信制御手段を介して利用者に提供する情報を蓄積しておく情報データベースと、秘密鍵と検査文を生成する情報提供者演算手段と、前記情報提供者通信制御手段を介して利用者端末との間で暗号通信を行なう情報提供者共通鍵暗号手段と、前記情報提供者通信制御手段を介して利用者の認証を行なう検証手段とを有することを特徴とする情報配送システムが提供される。

【００２３】

【作用】本発明によれば、第一に情報提供者による利用者の認証方法としてゼロ知識証明プロトコルを利用しているため、ゼロ知識証明プロトコルの目的や従来からの利用方法からいっても、利用者が正当なカードを利用していなければ情報提供者の検証をクリアし続けることはほとんど不可能であり、認証段階でほぼ完全に拒絶される。

【００２４】第二に情報提供者から配送情報を利用者へ配送する部分では、配送情報をゼロ知識証明プロトコルの検査文に含めて配送を行なっているため、ゼロ知識証明プロトコルが正常に終了すれば、カード上において間違いなく検査文、すなわち配送情報を受信・記録し、適正な処理をしていたことになる。また、途中で情報提供者の検証に失敗した場合にはそれ以降の認証は打ち切られ、残りの検査文は配送されないため、利用者が知ることのできる配送情報は検証に失敗する以前のものに限られる。

【００２５】第三に通信履歴を記録管理することにより情報提供者と利用者との間で正常な認証が行なわれたことを情報提供者は確認できるので、第二の効果と合わせて利用者は配送情報を受信し、かつカードの蓄積手段に配送情報が記録されているはずである。このことは、情報提供者から開示される通信履歴と利用者から提出されるカードに記録された配送情報とを照合することによって、利用者が情報暗号化用秘密鍵を生成できる状態であるかどうかを判定できる。なお、この場合、利用者からカードの提出がない場合には、情報暗号化用秘密鍵は生成できる状態にあると判定する。

【００２６】したがって、不正な利用者がシステムを利

用したり、あるいは配送情報のすべてを不正に搾取したりすることはできない。また、正常に認証が終了しているにも関わらず利用者が配送情報を受信していないなどという不当な主張に対して、情報提供者は通信履歴を開示するとともに、利用者にカードを提出するよう要求することにより対抗できる。

【００２７】

【実施例】以下、本発明の実施例を図面を用いて説明する。

【００２８】図２は、本発明の第１実施例における情報配送システムの構成例を示す図である。図２において、１は利用者が所有するカードであり、１１はカード固有の秘密情報を蓄積する秘密情報蓄積手段、１２はゼロ知識証明プロトコルで利用する乱数発生手段、１３はプロトコルを実行するうえで必要な演算を行う演算手段、１４は情報提供者からの情報を記録する蓄積手段である。なお、これらの手段はいずれもＩＣ等の耐タンパー装置上に組み込まれており、物理的に安全である。

【００２９】２は利用者が使用する固定型の利用者端末であり、２１はカード挿入手段、２２は情報提供者からの情報を蓄積する蓄積手段、２３は情報を利用する利用手段、２４は情報提供者との間で通信を行なうための通信制御手段である。

【００３０】３は利用者に配送情報の配送する情報提供者端末であり、３１は配送情報を蓄積する情報蓄積手段、３２は配送情報を分割して検査文の組を作成する情報分割手段、３３はゼロ知識証明プロトコルの検証を行なう検証手段、３４は通信履歴や認証記録を記録管理しておく履歴管理手段、３５は利用者端末との間で通信を行うための通信制御手段である。

【００３１】次に、図２のシステムにおけるゼロ知識証明プロトコルを利用した情報配送方法について、図３および図４に示す処理フローチャートと配送情報の例を基に説明する。なお、ここではゼロ知識証明プロトコルとしてFiat Shamir 法を用いることとし、準備段階として、信頼できるセンタが各利用者ごとにＰ，Ｑ，Ｎ，Ｉ，ｓを設定し、このうちＮとＩを利用者の公開情報として公開し、ｓを利用者の秘密情報としてカード１の秘密情報蓄積手段１１に蓄積して利用者に配布する。ここで、ＰとＱは互いに異なる大きな素数であり、Ｎ＝ＰＱである。また、$I = s^2 \pmod N$が成立している。

【００３２】情報暗号化用秘密鍵Ｗで暗号化されたメッセージＷ（ｍ）をすでに利用者端末２の蓄積手段２２に蓄積している利用者に対して、前記情報暗号化用秘密鍵Ｗを配送情報として配送する場合の例を説明する。

【００３３】まず、利用者は、自分のカード１をカード挿入手段２１に挿入後、情報提供者に情報暗号化用秘密鍵Ｗの配送を依頼する。（Ｓ１）。

【００３４】情報提供者は、情報蓄積手段３１に蓄積されている情報暗号化用秘密鍵Ｗを図４に示す配送情報５０のように情報分割手段３２においてｇビットごとに分割し、ｇビットで構成される検査文e_{ji}の組を作成する（Ｓ２）。ここで、情報暗号化用秘密鍵Ｗのビット数をL_wとすると、検査文の組はL_w/g個作成されることになり、ｉは１からｇまで、ｊは１からL_w/gまでの値をとる。

【００３５】次に、カード１は、乱数発生手段１２においてｇ個の乱数R_iを生成し（Ｓ３）、それぞれについて演算手段１３において$X_i = R_i^2 \pmod N$を計算し、X_iを通信制御手段２４を経由して情報提供者に送信する（Ｓ４）。

【００３６】通信制御手段３５を経由してX_iを受信した情報提供者は、ｊ組目の検査文e_{ji}を通信制御手段３５を経由してカード１に送信する（Ｓ５）。

【００３７】カード１では、通信制御手段２４を経由して受信した検査文e_{ji}のそれぞれのビットｉに対し、演算手段１３において０なら$Y_i = R_i$を、１なら秘密情報蓄積手段１１に蓄積されている秘密情報ｓを用いて$Y_i = sR_i \pmod N$を計算し、蓄積手段１４に検査文e_{ji}を記録した後、通信制御手段２４を経由してY_iを情報提供者に送信する（Ｓ６）。

【００３８】情報提供者は、通信制御手段３５を経由して受信した前記X_iと前記Y_i、および前記検査文e_{ji}からそれぞれのビットｉに対し、検証手段３３において検査ビットが０ならば検証式$Y_i^2 = X_i \pmod N$を、１ならば検証式$Y_i^2 = X_i I \pmod N$を満たすかどうかを検証する（Ｓ７）。この検証に失敗した場合には、カード１は不正であるとみなして、それ以降の利用を中止（Ｓ８）し、成功した場合には前記X_iと前記Y_i、および前記検査文e_{ji}を通信履歴として履歴管理手段３４に記録管理する（Ｓ９）。そして、上記Ｓ３以降のステップを情報分割手段３２で作成したL_w/g個の検査文e_{ji}の組すべてを送信し終わるまで繰り返し（Ｓ１０）、最終的に情報提供者は、情報分割手段３２で作成したL_w/g個の検査文e_{ji}の組すべての送信が終了した時点をもって情報暗号化用秘密鍵Ｗの配送が終了したとみなす（Ｓ１１）。

【００３９】カード１では蓄積手段１４に記録されたL_w/g個の検査文e_{ji}の組すべてを結合し、情報暗号化用秘密鍵Ｗを複製した（Ｓ１２）後、利用者端末２の利用手段２３に転送する（Ｓ１３）。利用手段２３では転送されてきた情報暗号化用秘密鍵Ｗを用いて蓄積手段２２に蓄積されている暗号化されたメッセージＷ（ｍ）を復号し、メッセージｍを得ることができる（Ｓ１４）。

【００４０】以上の説明は、利用者に対して確実に必要な情報を配送し、かつ利用者のカードに記録されたことを情報提供者が確認できるものである。例えば、メッセージｍを著作物などの有料情報とした時、情報暗号化用秘密鍵Ｗで暗号化したＷ（ｍ）をあらかじめ利用者に送信し、またはＣＤ－ＲＯＭ等の媒体に記録して配布して

おき、その後情報提供者が前記情報暗号化用秘密鍵Ｗを上記の配送方法によって送信することにより、メッセージｍを間違いなく購入した利用者に対して著作権使用料などの情報料を徴収するときに、情報提供者は履歴管理手段３４に記録管理された通信履歴を利用できる。また、電子メールにおいて郵便内容ｍを情報暗号化用秘密鍵Ｗで暗号化し、あらかじめ配達先にＷ（ｍ）を送信しておき、後日電子メール管理者から配達先に対して前記情報暗号化用秘密鍵Ｗを上記の配送方法により送信することにより、電子メール管理者は電子メールの配達証明に利用できるなど、さまざまな利用が可能である。

【００４１】以上説明したとおり、この第１実施例では、第一に情報提供者による利用者の認証方法としてゼロ知識証明プロトコルを利用しているため、ゼロ知識証明プロトコルの目的や従来からの利用方法からいっても、利用者が正当なカードを利用していなければ情報提供者の検証をクリアし続けることはほとんど不可能であり、認証段階でほぼ完全に拒絶される。

【００４２】第二に情報提供者から配送情報を利用者へ配送する部分では、配送情報をゼロ知識証明プロトコルの検査文に含めて配送を行なっているため、ゼロ知識証明プロトコルが正常に終了すれば、カード上において間違いなく検査文、すなわち配送情報を受信・記録し、適正な処理をしていたことになる。また、途中で情報提供者の検証に失敗した場合にはそれ以降の認証は打ち切られ、残りの検査文は配送されないため、利用者が知ることのできる配送情報は検証に失敗する以前のものに限られる。

【００４３】第三に通信履歴（前記X_i、前記Y_i、前記検査文e_{ji}）を記録管理することにより情報提供者と利用者との間で正常な認証が行なわれたことを情報提供者は確認できるので、第二の効果と合わせて利用者は配送情報を受信し、かつカードの蓄積手段１４に配送情報が記録されているはずである。このことは、情報提供者から開示される通信履歴と利用者から提出されるカードに記録された配送情報とを照合することによって、利用者が情報暗号化用秘密鍵Ｗを生成できる状態であるかどうかを判定できる。なお、この場合、利用者からカードの提出がない場合には、情報暗号化用秘密鍵Ｗは生成できる状態にあると判定する。

【００４４】したがって、不正な利用者がシステムを利用したり、あるいは配送情報のすべてを不正に搾取したりすることはできない。また、正常に認証が終了しているにも関わらず利用者が配送情報を受信していないなどという不当な主張に対して、情報提供者は通信履歴を開示するとともに、利用者にカードを提出するよう要求することにより対抗できる。

【００４５】なお当然のことであるが、上記の実施例においても、配送情報すべてを分割して検査文e_{ji}を生成する必要性はなく、例えば、配送情報の始めからｇｎビット目までを検査文e_{ji}（ｊ＝１，…，ｎ）とし、ｎ組の検査文e_{ji}によるゼロ知識証明プロトコルが終了した後、配送情報の残りの部分を一括して送信するような情報の配送方法も考えられる。この場合、ｎの値を様々に変えることにより、ゼロ知識証明におけるセキュリティレベルを変えられるうえ、通信量を削減できるといった特徴がある。例えばｎをL_s／ｇの半分とすれば、通信量もほぼ半分となる。

【００４６】また、検査文e_{ji}の生成方法についても、単純に配送情報を分割して生成するだけでなく、ダミー情報を付加したり、あるいは暗号化を行ったりして生成することも可能である。この場合、カード内にあらかじめ設定されている秘密情報、もしくは蓄積された検査文e_{ji}から自律的にダミー情報を除去、あるいは復号を行ったりして元の配送情報に復元する機能を持たせることにより、ゼロ知識証明を正常に終了しないかぎり、前記配送情報を取り出せないようにできる。したがって、第三者もしくは利用者が検査文e_{ji}を不正に搾取したり、大部分の検査文e_{ji}を受信した後、故意に認証を失敗させ、検査文e_{ji}のうち配送されてこない残りの部分を予測したりする等の不正行為を行ない、情報提供者が配送に失敗したと判断あるいは気がつかないうちに、第三者もしくは利用者が配送情報を獲得してしまうことがないようにできる。

【００４７】なお、上述の第１実施例による情報配送方法およびシステムでは、ゼロ知識証明プロトコルに必要な情報はすべて耐タンパー装置上に組み込まれており、実際の情報配送においても耐タンパー装置上に組み込まれた手段のみを用いて実行されるため、前記情報が外部に漏れることはなく、たとえカード所有者であっても前記情報を知ることができない。したがって、カード自体を偽造したり、あるいはカード上の記録情報を書き変えたりする等の不正行為を防止できる。

【００４８】次に本発明の第２実施例について説明する。

【００４９】図５は本発明の第２実施例における情報配送システムの構成を示すブロック図であり、１０は情報提供者端末２０から情報の提供を受ける利用者の端末（利用者端末）を示し、１００は通信回線３０を制御する通信制御手段、１０１は利用者の秘密情報を蓄積しておく利用者秘密情報蓄積手段、１０２は利用者が必要な情報を一時的に蓄積する一時メモリ、１０３は利用者が乱数を生成するための乱数発生手段、１０４は利用者が必要な演算を行う機能を有する演算手段、１０５は共通鍵暗号方法（例えば、ＤＥＳ，ＦＥＡＬ）による暗号通信を行うための共通鍵暗号手段、１０６は利用者が受信した情報を出力もしくは利用する情報出力／利用手段である。

【００５０】また、２０は情報を提供する情報提供者の端末（情報提供者端末）を示し、２００は通信回線３０

を制御する通信制御手段、２０１は情報提供者の秘密情報を蓄積しておく情報提供者秘密情報蓄積手段、２０２は提供する情報が蓄積してある情報データベース、２０３は情報提供者が必要な情報を一時的に蓄積する一時メモリ、２０４は情報提供者が必要な演算を行う機能を有する演算手段、２０５は共通鍵暗号方法による暗号通信を行うための共通鍵暗号手段、２０６はFiat Shamir 法に基づいて通信系列の正当性を検証する検証手段である。３０は利用者と情報提供者とを通信で接続する通信回線を表す。

【００５１】以下、図６のフローチャートにしたがって動作手順を説明する。

【００５２】まず基準段階として、信頼できるセンタが各利用者ごとにｐ１，ｑ１，Ｉ，ｓを設定し、このうちＮ１とＩを利用者の公開情報として公開し、ｓを利用者の秘密情報として利用者秘密情報蓄積手段１０１に蓄積して利用者に秘密裏に配布する。ここで、ｐ１とｑ１はそれぞれ互いに異なる大きな素数であり、Ｎ１＝ｐ１×ｑ１である。また、$I = s^2 \pmod{N1}$が成立している。

【００５３】さらに、各情報提供者と各利用者の間にはシステム秘密鍵ＳＫを設定し、利用者秘密情報蓄積手段１０１および情報提供者秘密情報蓄積手段２０１に登録しておく。このシステム秘密鍵ＳＫは、各情報提供者と各利用者の間ごとに異なる方が好ましいことはいうまでもないが、システム設計上、システム全体の共通鍵として１種類あるいは複数種類のシステム秘密鍵を複数の利用者で利用しても構わない。

【００５４】（１）配送確認ステップ

利用者端末１０は、乱数発生手段１０３によりｇ個の乱数R_i（ｉ＝１，２，…，ｇ）を生成し、一時メモリ１０２に蓄積し（Ｓ１０１）、その後、それぞれの乱数について演算手段１０４により初期応答文$X_i = R_i^2 \pmod{N1}$（ｉ＝１，２，…，ｇ）を計算し（Ｓ１０２）、通信回線３０を介して情報提供者端末２０に送信する（Ｓ１０３）。

【００５５】情報提供者端末２０は、受信した初期応答文X_i（ｉ＝１，２，…，ｇ）を一時メモリ２０３に蓄積し（Ｓ１０４）、その後、利用者端末１０に配送する情報Ｍを情報データベース２０２より取り出して（Ｓ１０５）、情報提供者秘密情報蓄積手段２０１に蓄積されたシステム秘密鍵ＳＫを秘密鍵として、共通鍵暗号手段２０５により暗号化した暗号文$C = E_{SK}(M)$を通信回線３０を介して利用者端末１０に送信する（Ｓ１０６）。

【００５６】利用者端末１０は、受信した暗号文Ｃを一時メモリ１０２に蓄積し（Ｓ１０７）、その後、演算手段１０４において暗号文Ｃを用いてｇビットの情報圧縮関数であるハッシュ関数ｈにより検査文$e_i = h(C)$（ｉ＝１，２，…，ｇ）を生成する（Ｓ１０８）。生成した検査文e_iのそれぞれのビットｉに対し、一時メモリ１０２に蓄積された乱数R_iと利用者秘密情報蓄積手段１０１に蓄積された利用者の秘密情報ｓとから$e_i = 0$ならば$Y_i = R_i$を、$e_i = 1$ならば$Y_i = sR_i \pmod{N1}$を計算し（Ｓ１０９）、応答文Y_i（ｉ＝１，２，…，ｇ）として情報提供者端末２０に通信回線３０を介して送信する（Ｓ１１０）。

【００５７】情報提供者端末２０は、受信した応答文Y_i（ｉ＝１，２，…，ｇ）を一時メモリ２０３に蓄積し（Ｓ１１１）、その後、演算手段２０４において暗号文Ｃを用いてｇビットの情報圧縮関数であるハッシュ関数ｈにより検査文$e_i = h(C)$（ｉ＝１，２，…，ｇ）を生成する（Ｓ１１２）。検証手段２０６において利用者の公開情報Ｉおよび一時メモリ２０３に蓄積された初期応答文X_iと応答文Y_iと検査文e_iとからそれぞれのビットｉに対し、$e_i = 0$ならば検証式$Y_i^2 = X_i \pmod{N1}$を、$e_i = 1$ならば検証式$Y_i^2 = X_i \times I \pmod{N1}$を満たすかどうかを検証する（Ｓ１１３）。この検証に失敗した場合には利用者は不正であると見做してそれ以降の利用を禁止し（Ｓ１１４Ａ）、成功した場合には情報Ｍの配送が正常に終了したと判断する（Ｓ１１４Ｂ）。

【００５８】（２）情報取り出しステップ

利用者端末１は、一時メモリ１０２に蓄積された暗号文Ｃを利用者秘密情報蓄積手段１０１に蓄積されたシステム秘密鍵ＳＫを秘密鍵として共通鍵暗号手段１０５により情報$M = D_{SK}(C)$に復号して、情報出力／利用手段１０６から情報Ｍを出力する（Ｓ１１５）。

【００５９】上記の情報配送方法を用いて配送確認ステップが正常に終了したことは、ゼロ知識証明プロトコルによる利用者認証が正常に行われたことのほかに、検査文e_i（ｉ＝１，２，…，ｇ）が正しく生成されたことの証明となる。また、検査文e_i（ｉ＝１，２，…，ｇ）は利用者端末１０が受信した暗号文Ｃより情報圧縮関数であるハッシュ関数を用いて生成されることから、正しい暗号文Ｃを受信しなければ正しい検査文e_i（ｉ＝１，２，…，ｇ）を生成することはできない。したがって、検査文e_i（ｉ＝１，２，…，ｇ）を利用者が正しく生成できることと、利用者が暗号文Ｃ（および情報Ｍ）を正常に受信したこととは同値となる。以上の説明から明らかなように、情報提供者は正確かつ確実に情報を利用者に配送したことを確認できる。

【００６０】なお、上記の説明において共通鍵暗号方法を利用して暗号化／復号を行なっているが、公開鍵暗号方法を利用しても当然構わない。また、Fiat Shamir 法をもとに説明したが、本方法は拡張Fiat Shamir 法（太田－岡本「Fiat-Shamir 法の高次への拡張」、電子情報通信学会技術研究報告ＩＳＥＣ８８－１３）を始めとする、素因数分解困難性あるいは離散対数問題等の困難性に安全性の根拠を置く全てのゼロ知識対話証明プロトコ

ルに応用が可能である。

【００６１】次に、本発明の第３実施例について説明する。

【００６２】図７は本発明の第３の実施例における情報配送システムの構成を示すブロック図であり、１０は情報提供者２０から情報の提供を受ける利用者の端末（利用者端末）を示し、構成手段は図５に示す第２実施例と同様である。２０は情報を提供する情報提供者の端末（情報提供者端末）を示し、２００から２０６までの構成手段は第２実施例と同様であり、２０７は情報任意ビット長の複数のブロックに分割し、蓄積する情報分割手段、２０８は後日情報を利用者に配送した事実を証明する証拠としての通信履歴を記録管理する通信履歴ファイルである。３０は第２実施例と同様に通信回線を表す。４０は後日、情報提供者が通信履歴ファイル２０８に記録管理している通信履歴について、中立的立場によりその通信履歴の正当性を判定する調停者の端末（調停者端末）を表し、４０１は必要な演算を行う機能を有する演算手段、４０２は調停者が必要な情報を一時的に蓄積する一時メモリ、４０３は正当性の判定を依頼された通信履歴についてその正当性を検証する検証手段、４０４は情報を任意ビット長の複数のブロックに分割し、蓄積する情報分割手段である。

【００６３】以下、図８のフローチャートにしたがって配送確認ステップでの動作手順を、また、図９のフローチャートにしたがって調停での動作手順を説明する。尚、準備段階は、前述した第２実施例と同様である。

【００６４】（１）配送確認ステップ

情報提供者端末２０は、利用者端末１０に配送する情報Ｍを情報データベース２０２から取り出し（Ｓ１２１）、情報分割手段２０７において情報Ｍを任意ビット長サイズの複数のブロックに分割し、情報ブロックMB_i（ｉ＝１，２，…，ｍ）として蓄積する（Ｓ１２２）。ここでは説明を簡単にするため、分割したブロック数をｍ、全てのブロックについビット長をｇで一定とする。

【００６５】これより以下の処理は第ｊブロックについてのものであり、第１ブロックから第ｍブロックまで各ブロックごとに以下の処理を順次（ｍ回）繰り返し行う。

【００６６】利用者端末１０は、乱数発生手段１０３によりｇ個の乱数R_{ij}（ｉ＝１，２，…，ｇ）を生成した後一時メモリ１０２に蓄積し（Ｓ１２３）、それぞれの乱数について演算手段１０４により初期応答文$X_{ij}=R_{ij}^2$ (mod Ｎ１)（ｉ＝１，２，…，ｇ）を計算した後一時メモリ１０２に蓄積する（Ｓ１２４）。その後、利用者秘密情報蓄積手段１０１に蓄積されているシステム秘密鍵ＳＫを秘密鍵として、共通鍵暗号手段１０５により暗号化した暗号化初期応答文$CX_{ij}=E_{SK}(X_{ij})$（ｉ＝１，２，…，ｇ）を通信回線３０を介して情報提供者端末２０に送信する（Ｓ１２５）。

【００６７】情報提供者端末２０は、受信した暗号化初期応答文CX_{ij}（ｉ＝１，２，…，ｇ）を情報提供者秘密情報蓄積手段２０１に蓄積されているシステム秘密鍵ＳＫを秘密鍵として、共通鍵暗号手段２０５により初期応答文$X_{ij}=D_{SK}(CX_{ij})$（ｉ＝１，２，…，ｇ）に復号して、一時メモリ２０３に蓄積する（Ｓ１２６）。その後、情報提供者秘密情報蓄積手段２０１に蓄積されているシステム秘密鍵ＳＫを秘密鍵として、情報分割手段２０７に蓄積された情報ブロックMB_jを共通鍵暗号手段２０５により暗号化した暗号文ブロック$CB_j=E_{SK}(MB_j)$を通信回線３０を介して利用者端末１０に送信する（Ｓ１２７）。

【００６８】利用者端末１０は、受信した暗号文ブロックCB_jを利用者秘密情報蓄積手段１０１に蓄積されているシステム秘密鍵ＳＫを秘密鍵として、共通鍵暗号手段１０５により情報ブロック$MB_j=D_{SK}(CB_j)$に復号して、情報出力／利用手段１０６から情報ブロックMB_jを出力する（Ｓ１２８）。

【００６９】さらに情報ブロックMB_jを出力すると同時に、演算手段１０４において情報ブロックMB_jと一時メモリ１０２に蓄積された初期応答文X_{ij}（ｉ＝１，２，…，ｇ）とを用いて一方向性ランダムハッシュ関数ｈにより検査文$e_{ij}=h(MB_j \| X_{1j} \| X_{2j} \| \cdots \| X_{gj})$（ｉ＝１，２，…，ｇ）を生成し（Ｓ１２９）、生成した検査文e_{ij}のそれぞれのビットｉに対し、一時メモリ１０２に蓄積された乱数R_{ij}と利用者秘密情報蓄積手段１０１に蓄積された利用者の秘密情報ｓとから$e_{ij}=0$ならば$Y_{ji}=R_{ij}$を、$e_{ij}=1$ならば$Y_{ji}=sR_{ij}$ (mod Ｎ１)を計算して（Ｓ１３０）、応答文Y_{ij}（ｉ＝１，２，…，ｇ）として情報提供者端末２０に通信回線３０を介して送信する（Ｓ１３１）。

【００７０】情報提供者端末２０は、受信した応答文Y_{ij}（ｉ＝１，２，…，ｇ）を一時メモリ２０３に蓄積し（Ｓ１３２）、その後、演算手段２０４において一時メモリ２０３に蓄積された初期応答文X_{ij}（ｉ＝１，２，…，ｇ）と情報分割手段２０７に蓄積された情報ブロックMB_jとを用いて、一方向性ランダムハッシュ関数ｈにより検査文$e_{ij}=h(MB_j \| X_{1j} \| X_{2j} \| \cdots \| X_{gj})$（ｉ＝１，２，…，ｇ）を生成し、一時メモリ２０３に蓄積する（Ｓ１３３）。

【００７１】そして、検証手段２０６において利用者の公開情報Ｉおよび一時メモリ２０３に蓄積された初期応答文X_{ij}と応答文Y_{ij}と検査文e_{ij}とからそれぞれのビットｉに対し、$e_{ij}=0$ならば検証式$Y_{ij}^2=X_{ij}$ (mod Ｎ１)を、$e_{ij}=1$ならば検証式$Y_{ij}^2=X_{ij}\times I$ (mod Ｎ１)を満たすかどうかを検証する（Ｓ１３４）。この検証に失敗した場合には利用者は不正であると見做して直ちにプロトコルの実行を中止し（Ｓ１３５）、成功した場合には全てのブロックが終了するまで

以上の処理を繰り返す（Ｓ１３６）。そして、第１ブロックから第ｍブロックまでの全てのブロックについて検証に成功した場合には、一時メモリ２０３に蓄積された情報Ｍ、検査文e_{ij}、応答文Y_{ij}（ｉ＝１，２，…，ｇ：ｊ＝１，２，…，ｍ）を通信履歴Ｈとして通信履歴ファイル２０８に記録管理する（Ｓ１３７）。

【００７２】（２）調停

後日、利用者が情報Ｍを受信していないと主張した場合には、情報提供者端末２０は通信履歴ファイル２０８に記録管理された通信履歴Ｈを提示し、調停者端末４０の一時メモリ４０２に蓄積する（Ｓ１４１）。

【００７３】調停者端末４０は、情報分割手段４０４において、一時メモリ４０２に蓄積された通信履歴中の情報Ｍについて、情報Ｍを複数の情報ブロックMB_j（ｊ＝１，２，…，ｍ）に分割して蓄積する（Ｓ１４２）。

【００７４】各ブロック（第ｊブロック）について、演算手段４０１において利用者端末１０の公開情報Ｉと一時メモリ４０２に蓄積された通信履歴Ｈ中の検査文e_{ij}および応答文Y_{ij}からそれぞれのビットｉに対し、$e_{ij}=0$ならば$Y_{ij}=Y_{ij}^2 \pmod{N1}$を、$e_{ij}=1$ならば$X_{ij}=Y_{ij}^2/I \pmod{N1}$を計算し、計算結果$X_{ij}$（ｉ＝１，２，…，ｇ）を一時メモリ４０２に蓄積する（Ｓ１４３）。

【００７５】次に、情報分割手段４０４に蓄積された情報ブロックMB_jと一時メモリ４０２に蓄積された計算結果X_{ij}（ｉ＝１，２，…，ｇ）とから演算手段４０１の一方向性ランダムハッシュ関数ｈにより検査文$e_{ij}=h(MB_j \| X_{1j} \| X_{2j} \| \cdots \| X_{gj})$（ｉ＝１，２，…，ｇ）を生成する。（Ｓ１４４）。

【００７６】その後、検証手段４０３において一時メモリ４０２に蓄積された通信履歴Ｈ中の検査文e_{ij}（ｉ＝１，２，…，ｇ）と一致するかどうかを検査する（Ｓ１４５）。全てのブロック（第１ブロックから第ｍブロックまでのｍブロック）について一致すれば（Ｓ１４６）、通信履歴Ｈの正当性が保証されたこととなり（Ｓ１４７）、そうでなければ通信履歴Ｈは無効となる（Ｓ１４８）。

【００７７】上記の情報配送方法を用いて配送確認ステップが正常に終了したことは、ゼロ知識証明プロトコルによる利用者認証が正常に行われたことのほかに、検査文e_{ij}（ｉ＝１，２，…，ｇ：ｊ＝１，２，…，ｍ）が正しく生成されたことの証明となる。また、検査文e_{ij}（ｉ＝１，２，…，ｇ：ｊ＝１，２，…，ｍ）は利用者が受信した情報ブロックMB_j（ｊ＝１，２，…，ｍ）と利用者が生成した初期応答文X_{ij}（ｉ＝１，２，…，ｇ：ｊ＝１，２，…，ｍ）とから一方向性ランダムハッシュ関数ｈを用いて生成されることから、正しい情報ブロックMB_j（ｊ＝１，２，…，ｍ）を受信しなければ正しい検査文e_{ij}（ｉ＝１，２，…，ｇ：ｊ＝１，２，…，ｍ）を生成することはできない。したがって、検査文e_{ij}（ｉ＝１，２，…，ｇ：ｊ＝１，２，…，ｍ）を利用者が正しく生成できることと利用者が情報ブロックMB_j（ｊ＝１，２，…，ｍ）を正常に受信したこととは同値となる。したがって、情報提供者は正確かつ確実に情報を利用者に配送したことを確認できる。

【００７８】なお、上記の説明では、共通鍵暗号方法を利用して暗号化／復号を行った例を説明したが、公開鍵暗号方法を利用しても当然構わない。また、Fiat Shamir 法をもとに説明をしたが、本方法は拡張Fiat Shamir 法（太田－岡本「Fiat-Shamir 法の高次への拡張」、電子情報通信学会技術研究報告ＩＳＥＣ８８－１３）を始めとする、素因数分解困難性あるいは離散対数問題等の困難性に安全性の根拠を置く全てのゼロ知識対話証明プロトコルに対応が可能である。

【００７９】次に、検査文e_{ij}、応答文Y_{ij}、（ｉ＝１，２，…，ｇ：ｊ＝１，２，…，ｍ）、情報Ｍからなる通信履歴Ｈの関係では、ゼロ知識証明プロトコルにおける検証式と一方向性ランダムハッシュ関数とにより相互に関係し合っているため、一部を不正に改竄するなどして通信履歴Ｈを偽造することは不可能である。したがって、通信履歴Ｈを記録管理することにより、情報Ｍを利用者が確実に受信していることの証拠として、後日、調停者などの中立的な第三者に提示することができる。

【００８０】さらに、情報提供者端末と利用者端末との間の通信が情報Ｍの分割ブロック数ｍと同じ回数だけ繰り返し行われるため、途中で情報提供者の検証に失敗した場合にはそれ以降の通信は打ち切られ、残りの情報ブロックは送信されない。すなわち、利用者が知ることのできる情報ブロックは検証に失敗する以前のもののみに限られるので、情報提供者の検証を失敗させた利用者は結果として情報Ｍ全体を正しく受信することが不可能となる。したがって、利用者の秘密情報ｓを知らない不正な利用者が不正な応答文Y_{ij}（ｉ＝１，２，…，ｇ）を送信する場合はもとより、応答文そのものを送信しないような不正行為を行い、情報提供者が情報Ｍを利用者に配送した事実を証明する通信履歴Ｈを情報提供者が記録管理できないにもかかわらず、利用者が情報Ｍ全体を不正に獲得してしまうことがないようにすることが可能である。

【００８１】また、上記の説明では分割するブロックを各ブロックともビット長をｇで一定としたが、例えば第１ブロックは１ビット、第２ブロックは２ビット、第３ブロックは４ビットというようにブロックごとにビット長サイズを変えても当然構わない。

【００８２】以上の説明は、情報提供者が情報Ｍを正確かつ確実に利用者に配送したことを証明できるものであり、例えば著作物などの有料情報を情報Ｍとして配送する場合、あるいはあらかじめ暗号化されたソフトウェアなどをＣＤ－ＲＯＭ等により無償あるいは有償で配布した後、暗号化されたソフトウェアを復号するための鍵を

情報Mとして配送する場合、上記の情報配送方法によって情報提供者が利用者に情報Mを配送することにより、情報提供者が記録管理する通信履歴Hを著作権使用料等の情報料あるいはソフトウェアの販売代金を徴収するときの証明情報として利用できるなど、様々な利用が可能である。

【００８３】次に、本発明の第４実施例について説明する。

【００８４】図１０は本発明の第４実施例における情報配送システムの構成を示すブロック図であり、１０は情報提供者端末２０から情報の提供を受ける利用者の端末（利用者端末）を示し、１００から１０６までは第２実施例と同様の構成であり、１０７は公開鍵暗号方法（例えば、ＲＳＡ，ElGamal ）による暗号通信を行うための公開鍵暗号手段、１０８は分割されたブロック情報を元の情報再構成する情報再構成手段、１０９は情報提供者から受信した情報を蓄積する情報蓄積手段である。２０は情報を提供する情報提供者の端末（情報提供者端末）を示し、２００から２０８までは第３実施例と同様の構成であり、２０９は情報提供者が乱数を生成するための乱数発生手段、２１０は公開鍵暗号方法による暗号通信を行うための公開鍵暗号手段である。３０は第２実施例と同様に通信回線である。４０は調停者端末を表し、４０１から４０４までは第３実施例と同様の構成であり、４０５は公開鍵暗号方法による暗号化を行うための公開鍵暗号手段である。

【００８５】以下、図１１のフローチャートにしたがって配送確認ステップと情報取り出しステップでの動作手順を、また図１２のフローチャートにしたがって調停での動作手順を説明する。

【００８６】まず、準備段階として、信頼できるセンタが各利用者ごとにｐ１，ｑ１，Ｉ，ｓ，ｐ２，ｑ２，ＰＵ，ＳＵを設定し、このうちＮ１，Ｎ２，Ｉ，ＰＵを利用者の公開情報（公開鍵）として公開し、ｓ，ＳＵを利用者の秘密情報（秘密鍵）として利用者秘密情報蓄積手段１０１に蓄積して利用者に秘密裏に配布する。ここで、（ｐ１，ｑ１）と（ｐ２，ｑ２）の各組はそれぞれ互いに異なる大きな素数の組になっており、Ｎ１＝ｐ１×ｑ１、Ｎ２＝ｐ２×ｑ２である。また、$I = s^2 \pmod{N1}$，$PU \times SU = 1 \pmod{(p2-1)(q2-1)}$が成立している。なお、ｐ１＝ｐ２，ｑ１＝ｑ２としてもよい。

【００８７】（１）配送確認ステップ

利用者端末１０は、乱数発生手段１０３によりｇ×ｍ個の乱数R_{jk}（ｊ＝１，２，…，ｇ：ｋ＝１，２，…，ｍ）を生成し、一時メモリ１０２に蓄積する（Ｓ１５１）。それぞれの乱数について演算手段１０４により初期応答文$X_{jk} = R_{jk}^2 \pmod{N1}$（ｊ＝１，２，…，ｇ：ｋ＝１，２，…，ｍ）を計算し（Ｓ１５２）、通信回線３０を介して情報提供者に送信する（Ｓ１５３）。

【００８８】情報提供者端末２０は、受信した初期応答文X_{jk}（ｊ＝１，２，…，ｇ：ｋ＝１，２，…，ｍ）を一時メモリ２０３に蓄積し（Ｓ１５４）、また乱数発生手段２０９により乱数文Ｚをランダムに生成して一時メモリ２０３に蓄積する（Ｓ１５５）。

【００８９】次に、初期応答文X_{jk}（ｊ＝１，２，…，ｇ：ｋ＝１，２，…，ｍ）と乱数文Ｚとから演算手段２０４の一方向性ランダムハッシュ関数ｈによりｇビットサイズの情報暗号化用秘密鍵$W_j = h(Z \| X_{11} \| X_{21} \| \cdots \| X_{gm})$（ｊ＝１，２，…，ｇ）を生成して一時メモリ２０３に蓄積する（Ｓ１５６）。ここで、一般にｇの値は共通鍵暗号手段１０５および共通鍵暗号手段２０５で使用する秘密鍵の鍵長と等しいかそれ以上である。その後、配送する情報Mを情報データベース２０２から取り出し（Ｓ１５７）、情報暗号化用秘密鍵W_j（ｊ＝１，２，…，ｇ）を秘密鍵として共通鍵暗号手段２０５により暗号文$C = E_{\blacktriangledown}(M)$に暗号化した後、利用者端末１０に暗号文Ｃを通信回線３０を介して送信する（Ｓ１５８）。

【００９０】利用者端末１０は、暗号文Ｃを情報蓄積手段１０９に受信／蓄積した後、受信した旨を通信回線３０を介して情報提供者端末２０に通知する（Ｓ１５９）。

【００９１】情報提供者端末２０は、一時メモリ２０３に蓄積された情報暗号化用秘密鍵W_j（ｊ＝１，２，…，ｇ）を利用者の公開情報ＰＵを用いて公開鍵暗号手段２１０により暗号化して検査文$e_i = (W_1 \| W_2 \| \cdots \| W_g)^{PU} \pmod{N2}$（ｉ＝１，２，…，Ｌ）を生成する（Ｓ１６０）。なお、ＬはＮ２のビット長に等しい。

【００９２】次に、情報分割手段２０７において検査文e_i（ｉ＝１，２，…，Ｌ）を複数個のブロックに分割し、検査文ブロックとして蓄積する（Ｓ１６１）。ここでは説明を簡単にするため、分割したブロック数をｍ、全てのブロックについてビット長をｇで一定とし、分割した検査文を検査文ブロックeB_{jk}（ｊ＝１，２，…，ｇ：ｋ＝１，２，…，ｍ）と表す。すなわち、$eB_{jk} = e_{(j+g(k-1))}$であり、例えば$eB_{11} = e_1$，$eB_{g1} = e_g$，$eB_{12} = e_{g+1}$，$eB_{Lm} = e_L$のようになる。

【００９３】これより以下の処理は第ｋブロックについてのものであり、第１ブロックから第ｍブロックまで各ブロックごとに以下の処理を順次（ｍ回）繰り返し行う。

【００９４】情報提供者端末２０は、情報分割手段２０７に蓄積された検査文ブロックeB_{jk}（ｊ＝１，２，…，ｇ）を通信回線３０を介して利用者端末１０に送信する（Ｓ１６２）。

【００９５】利用者端末１０は、受信した検査文ブロックeB_{jk}（ｊ＝１，２，…，ｇ）を一時メモリ１０２に蓄積し（Ｓ１６３）、その後、演算手段１０４において

受信した検査文ブロックeB_{jk}のそれぞれのビットｊに対し、一時メモリ１０２に蓄積された乱数R_{jk}と利用者秘密情報蓄積手段１０１に蓄積された利用者の秘密情報ｓとから$eB_{jk}=0$ならば$Y_{jk}=R_{jk}$を、$eB_{jk}=1$ならば$Y_{jk}=sR_{jk}$（mod Ｎ１）を計算して（Ｓ１６４）、応答文Y_{jk}（ｊ＝１，２，…，ｇ）として情報提供者端末２０に通信回線３０を介して送信する（Ｓ１６５）。

【００９６】情報提供者端末２０は、受信した応答文Y_{jk}（ｊ＝１，２，…，ｇ）を一時メモリ２０３に蓄積し（Ｓ１６６）、その後、検証手段２０６において利用者の公開情報Ｉおよび一時メモリ２０３に蓄積された初期応答文X_{jk}と応答文Y_{jk}と検査文e_{jk}とからそれぞれのビットｊに対し、$e_{jk}=0$ならば検証式$Y_{jk}^{2}=X_{jk}$（mod Ｎ１）を、$e_{jk}=1$ならば検証式$Y_{jk}^{2}=X_{jk}\times I$（mod Ｎ１）を満たすかどうかを検証する（Ｓ１６７）。この検証に失敗した場合には利用者は不正であると見做して直ちにプロトコルの実行を中止し（Ｓ１６８）、成功した場合には全てのブロックが終了するまで以上の処理を繰り返す（Ｓ１６９）。そして、第１ブロックから第ｍブロックまでの全てのブロックについて検証に成功した場合には、一時メモリ２０３に蓄積された乱数文Ｚ、検査文e_{jk}、応答文Y_{jk}（ｊ＝１，２，…，ｇ：ｋ＝１，２，…，ｍ）を通信履歴Ｈとして通信履歴ファイル２０８に記録管理する（Ｓ１７０）。

【００９７】（２）情報取り出しステップ

利用者端末１０は、情報再構成手段１０８において、一時メモリ１０２に蓄積された検査文ブロックeB_{jk}（ｊ＝１，２，…，ｇ：ｋ＝１，２，…，ｍ）から検査文e_{i}（ｉ＝１，２，…，Ｌ）を再構成し（Ｓ１７１）、利用者秘密情報蓄積手段１０１に蓄積されている利用者の秘密情報ＳＵを用いて公開鍵暗号手段１０７により復号して情報暗号化用秘密鍵$W_{j}=(e_{1}\|e_{2}\|\cdots\|e_{L})^{SU}$（mod Ｎ２）（ｊ＝１，２，…，ｇ）を獲得した後、情報蓄積手段１０９に蓄積する（Ｓ１７２）。

【００９８】最後に、情報蓄積手段１０９に蓄積された情報暗号化用秘密鍵W_{j}（ｊ＝１，２，…，ｇ）を秘密鍵として、共通鍵暗号手段１０５により情報蓄積手段１０９に蓄積された暗号文Ｃを復号し、情報Ｍ＝Ｄ（Ｃ）を情報出力／利用手段１０６より獲得することができる（Ｓ１７３）。

【００９９】（３）調停

後日、利用者が情報Ｍを受信していないと主張した場合には、情報提供者端末２０は通信履歴ファイル２０８に記録管理された通信履歴Ｈを提示し、調停者端末４０の一時メモリ４０２に蓄積する（Ｓ１８１）。

【０１００】調停者端末４０は、各ブロック（第ｋブロック）について一時メモリ４０２に蓄積された通信履歴Ｈ中の検査文e_{jk}および応答文Y_{jk}からそれぞれのビットｊに対し、演算手段４０１において$e_{jk}=0$ならば$X_{jk}=Y_{jk}^{2}$（mod Ｎ１）を、$e_{jk}=1$ならば$X_{jk}=Y_{jk}^{2}/I$（mod Ｎ１）を計算し、計算結果X_{jk}（ｊ＝１，２，…，ｇ）を一時メモリ４０２に蓄積する（Ｓ１８２）。

【０１０１】次いで、一時メモリ４０２に蓄積された計算結果X_{jk}（ｊ＝１，２，…，ｇ）と乱数文Ｚとを用いて演算手段４０１の一方向性ランダムハッシュ関数ｈによりｇビットサイズの情報暗号化用秘密鍵$W_{j}=h(Z\|X_{11}\|X_{21}\|\cdots\|X_{gn})$（ｊ＝１，２，…，ｇ）を生成し（Ｓ１８３）、利用者の公開情報ＰＵを用いて公開鍵暗号手段４０５により暗号化して検査文$e_{i}=(W_{1}\|W_{2}\|\cdots\|W_{g})^{PU}$（mod Ｎ２）（ｉ＝１，２，…，Ｌ）を生成する（Ｓ１８４）。

【０１０２】その後、情報分割手段４０４において検査文e_{i}（ｉ＝１，２，…，Ｌ）を複数個のブロックに分割して、検査文ブロックeB_{jk}（ｊ＝１，２，…，ｇ：ｋ＝１，２，…，ｍ）生成し（Ｓ１８５）、最後に各ブロック（第ｋブロック）について、検証手段４０３において一時メモリ４０２に蓄積された通信履歴Ｈ中の検査文e_{jk}（ｊ＝１，２，…，ｇ）と一致するかどうかを検査する（Ｓ１８６）。全てのブロック（第１ブロックから第ｍブロックまでのｍブロック）について一致すれば（Ｓ１８７）、通信履歴Ｈの正当性が証明されたことになり、利用者が情報Ｍを受信していることが保証されたこととなり（Ｓ１８８）、そうでなければ通信履歴Ｈは無効とされる（Ｓ１８９）。

【０１０３】上記の情報配送方法を用いれば、情報Ｍ本体は初めに暗号文Ｃに暗号化されて利用者に送信されるため、暗号文Ｃを利用者が受信した時点では情報Ｍを獲得されることはない。そして、ゼロ知識証明プロトコルが正常に終了した時点で、ゼロ知識証明プロトコルによる利用者認証が正常に行われたことのほかに、検査文e_{jk}（ｊ＝１，２，…，ｇ：ｋ＝１，２，…，ｍ）を利用者が正しく受信したことの証明となる。

【０１０４】また、検査文e_{jk}（ｊ＝１，２，…，ｇ：ｋ＝１，２，…，ｍ）を利用者が復号することにより情報暗号化用秘密鍵W_{j}（ｊ＝１，２，…，ｇ）を生成し、生成した情報暗号化用秘密鍵W_{j}（ｊ＝１，２，…，ｇ）を用いて暗号文Ｃを復号して情報Ｍを獲得することができる。したがって、検査文e_{jk}（ｊ＝１，２，…，ｇ：ｋ＝１，２，…，ｍ）を利用者が正しく受信したことと利用者が情報Ｍを正常に受信したこととは同値となる。したがって、情報提供者は正確かつ確実に情報を利用者に配送したことを確認できる。

【０１０５】なお、上記の説明において公開鍵暗号方法を利用して暗号化／復号を行っているが、共通鍵暗号方法を利用しても当然構わない。また、Fiat Shamir 法をもとに説明したが、本方法は拡張Fiat Shamir 法（太田－岡本「Fiat-Shamir 法の高次への拡張」、電子情報通信学会技術研究報告ＩＳＥＣ８８－１３）を始めとす

る、素因数分解困難性あるいは離散対数問題等の困難性に安全性の根拠を置く全てのゼロ知識対話証明プロトコルに応用が可能である。

【0106】次に、検査文e_{jk}、応答文Y_{jk}、（j＝1，2，…，g：k＝1，2，…，m）、乱数文Zからなる通信履歴Hの関係では、ゼロ知識証明プロトコルにおける検証式と一方向性ランダムハッシュ関数とにより相互に関係し合っているため、一部を不正に改竄するなどして通信履歴Hを偽造することは不可能である。したがって、通信履歴Hを記録管理することにより、情報暗号化用秘密鍵W_j（j＝1，2，…，g）を利用者が確実に受信していることの証拠として、後日、調停者などの中立的な第三者に提示することができる。

【0107】さらに、情報提供者と利用者との間の通信が情報暗号化用秘密鍵W_j（j＝1，2，…，g）の分割ブロック数mと同じ回数だけ繰り返し行われるため、途中で情報提供者の検証に失敗した場合にはそれ以降の通信は打ち切られ、残りの検査文は送信されない。すなわち、利用者が知ることのできる検査文は検証に失敗する以前のもののみに限られるので、情報提供者の検証を失敗させた利用者は暗号文Cを復号するために必要な情報の一部しか獲得することができず、結果として正しい情報暗号化用秘密鍵W_j（j＝1，2，…，g）を生成することが不可能となる。したがって、利用者の秘密情報sを知らない不正な利用者が不正な応答文Y_{jk}（j＝1，2，…，g：k＝1，2，…，m）を送信する場合はもとより、応答文そのものを送信しないような不正行為を行い、情報提供者が情報Mを利用者に配送した事実を証明する通信履歴Hを情報提供者が記録管理できないにもかかわらず、利用者が情報Mを獲得するのに必要な検査文e_{jk}（j＝1，2，…，g：k＝1，2，…，m）を受信し、情報Mを不正に復号／獲得してしまうことがないようにすることが可能である。また、上記の説明では分割するブロックを各ブロックともビット長をgで一定としたが、例えば第1ブロックは1ビット、第2ブロックは2ビット、第3ブロックは4ビットというようにブロックごとにビット長サイズを変えても当然構わない。

【0108】以上の説明は、情報提供者が大容量の情報Mを正確かつ確実に利用者に配送したことを証明できるものであり、例えば情報Mを著作物などの「オンデマンドサービス」としての有料情報とした場合、上記の情報配送方法によって情報提供者が利用者に情報Mを配送することにより、情報提供者が記録管理する通信履歴Hを著作権使用料等の情報料を徴収するときの証明情報として利用できるなど、様々な利用が可能である。

【0109】以上説明したとおり、本発明の第2～第4実施例のゼロ知識証明プロトコルを利用した情報配送方法では、第一にプロトコルの動作自体は利用者認証としてのゼロ知識証明プロトコルと同等であるため、ゼロ知識証明プロトコルと同様に、不正な利用者が情報提供者の検証をクリアすることはほぼ不可能である。第二に配送確認ステップが正常に終了した場合には、ゼロ知識証明プロトコルが正常に終了したことと同値であるので、情報提供者は正しい利用者が情報を正しく受信していると判断できる。

【0110】又、情報を暗号化し暗号文として送信することにより、第三者による情報の盗聴を防止し、かつ第三者が情報を解読するために有効な情報も得られないようにすることもできる。

【0111】又、本発明の第2実施例によれば、暗号文の復号処理を配送確認ステップと切り離して実行することができる。

【0112】又、本発明の第2、第3実施例によれば、例えばハッシュ関数などを用いて情報（または利用者が復号可能な暗号文）から検査文を生成することにより検査文のサイズを小さくすることができ、配送確認ステップにおける通信量及び処理時間を削減できる。

【0113】又、本発明の第3実施例によれば、一方向性関数を用いて検査文を生成することにより、情報（または利用者が復号可能な暗号文）、応答文、及び検査文とからなる通信履歴の偽造を不可能にする。

【0114】又、例えば不正な利用者による利用などにより配送確認ステップの途中で情報提供者のプロトコルに失敗した場合には、直ちにプロトコルの実行が中止され、検証に失敗した以降のブロックは利用者に送信されないことになるため、結果として情報（または利用者が復号可能な暗号文）全てを不正に獲得してしまうことがないようにできる。

【0115】又、本発明の第4実施例によれば、大容量の情報を送信する場合に、第一に情報は情報提供者が生成した情報暗号化用秘密鍵によって初めに暗号化されて利用者に配送されるため、利用者の認証が行われる以前に情報本体を利用者が取り出すことはできない。第二に情報暗号化用秘密鍵についてのみ検査文として配送確認を行うことにより、通信量及び配送確認のための処理時間を大幅に短縮できる。第三に配送確認ステップが正常に終了すれば利用者は検査文を正しく受信したことが確認でき、情報取り出しステップにおいて情報暗号化用秘密鍵を獲得することが保証されるので、この時点で初めて情報を間違いなく取り出すことができる。したがって、これらの効果により情報配送方法が終了した場合には、情報提供者は正規の利用者に対して情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送し、かつ確実に利用者が受信したことが確認できるので、情報提供者は情報を利用者まで確実に配送したと判断できる。

【0116】又、一方向性関数を用いて情報暗号化用秘密鍵を生成することにより情報提供者にとって都合の良い情報暗号化用秘密鍵を不正に生成できないようにする

ことができる。また、同様に一方向性関数を用いることにより、乱数文と検査文と応答文とからなる通信履歴を偽造することは不可能になるので、情報提供者は正規の利用者に対して要求された情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送し、かつ確実に利用者が受信したことを後日証明できる証拠能力を持つことができる。

【０１１７】又、検査文について暗号通信を行うことは、情報暗号化用秘密鍵についても暗号通信を行なっていることと同等の効果が得られるため、第三者による情報暗号化用秘密鍵の盗聴を防止し、かつ第三者が情報暗号化用秘密鍵を解読するために有効な情報も得られないようにもなる。

【０１１８】又、検査文の復号処理を配送確認ステップと切り離して実行することができる。

【０１１９】又、例えば不正な利用者による利用などにより配送確認ステップの途中で情報提供者の検証に失敗した場合には、ただちにプロトコルの実行が中止され、検証に失敗した以降のブロックは利用者に送信されないことになる。したがって、情報提供者の検証を失敗させた利用者は暗号化された情報を復号するために必要な情報の一部しか獲得することができず、結果として情報本体もしくは情報暗号化用秘密鍵を生成することが不可能となるので、不正な利用者が要求した情報を不正に獲得してしまうことがないようにできる。

【０１２０】又、本発明の第３、第４実施例によれば、偽造不可能な通信履歴を実際に情報を配送した証拠として記録管理することができ、かつ必要に応じて提示できるようになる。さらに、情報提供者が情報を配送した事実の証拠として記録管理しなければならない情報量が桜井（特開平５－１２３２１）の方式と比較して大幅に削減できる。

【０１２１】又、情報提供者と利用者の間で情報の提供の有無について調停を行う必要が生じた場合、情報提供者が通信履歴を裁判所等の中立な調停機関に提示し、調停機関が証拠能力を有する通信履歴についてその正当性を検査することにより、情報提供者と利用者のどちらの主張が正当であるのかを判定できる。すなわち、情報提供者が利用者に対して情報（または利用者が復号可能な暗号文）を送信し、かつ利用者が確実に受信したことを、後日調停者が確認できるので、利用者が情報（または利用者が復号可能な暗号文）を受信しているにも関わらず、利用者が情報を受信していないなどという不当な主張を防止できる。

【０１２２】又、これらの実施例によれば、情報提供者が要求された情報を利用者に確実に配送し、かつ利用者が確実に受信していることを情報提供者が確認できるシステムとなる。また、必要に応じて情報提供者が利用者を認証する利用者認証方法としてのゼロ知識証明プロトコルを単独に使用することもできる。

【０１２３】又、情報提供者と利用者の間で暗号通信ができるようにしたシステムとなる。

【０１２４】又、本発明の第４実施例によれば、情報提供者から提供された情報を蓄積し、利用者が必要に応じて情報を利用できるようにしたシステムとなる。

【０１２５】又、情報暗号化用秘密鍵の生成機能を有し、情報暗号化用秘密鍵を用いた情報配送ができようにしたシステムとなる。

【０１２６】又、本発明の第３、第４実施例によれば、証拠能力を有する通信履歴を必要に応じて提示できるようにしたシステムとなる。

【０１２７】又、不正な利用者であることを検出した際には直ちにプロトコルの実行を中止して、不正な利用者が要求した情報を不正に獲得してしまうことがないようにしたシステムとなる。

【０１２８】又、裁判所等の中立な調停機関により、証拠能力を有する通信履歴についてその正当性を検査し、情報提供者と利用者のどちらの主張が正当であるのかを判定することができるようにしたシステムとなる。

【０１２９】次に本発明の第５実施例について説明する。

【０１３０】図１３は本発明の第５実施例における情報配送システムの構成を示すブロック図であり、１０は情報提供者に対して情報の配送を必要とする利用者（端末）を示し、１００は通信回線３０を制御する通信制御手段、１０１はセンタが作成し利用者の秘密情報を蓄積しておく利用者秘密情報蓄積手段、１０５は共通鍵暗号方法（例えば、ＤＥＳ，ＦＥＡＬ）による暗号通信を行うための共通鍵暗号手段、１０７は公開鍵暗号方法（例えば、ＲＳＡ）による暗号通信を行うための公開鍵暗号手段、１０９は情報提供者から配送された情報を蓄積する情報蓄積手段、１０２は利用者が必要な情報を一時的に蓄積する一時メモリ、１０３は利用者が乱数を生成するための乱数発生手段、１０４は必要な演算を行う演算手段、１０６は利用者が要求した情報を出力もしくは利用する情報出力／利用手段である。

【０１３１】また、２０は情報を提供する情報提供者（端末）を示し、２００は通信回線３０を制御する通信制御手段、２０１はセンタが作成した情報提供者の秘密情報を蓄積しておく情報提供者秘密情報蓄積手段、２０５は共通鍵暗号方法による暗号通信を行うための共通鍵暗号手段、２１０は公開鍵暗号方法による暗号通信を行うための公開鍵暗号手段、２０２は提供する情報が蓄積してある情報データベース、２０３は情報提供者が必要な情報を一時的に蓄積する一時メモリ、２０９は情報提供者が乱数を生成するための乱数発生手段、２０４は必要な演算を行う演算手段、２０６はFiat Shamir 法に基づいて通信系列の正当性を検証する検証手段である。３０は利用者と情報提供者とを通信で接続する通信回線を表す。

【０１３２】以下、図１４のフローチャートにしたがって情報配送ステップ、配送確認ステップ、情報取り出しステップの動作手順を説明する。

【０１３３】まず基準段階として、信頼できるセンタが各利用者ごとにｐ１，ｑ１，Ｉ，ｓ，ｐ２，ｑ２，ＰＵ，ＳＵを設定し、このうちＮ１，Ｎ２，Ｉ，ＰＵを利用者の公開情報（公開鍵）として公開し、ｓ，ＳＵを利用者の秘密情報（秘密鍵）として利用者秘密情報蓄積手段１０１に蓄積して利用者に秘密裏に配布する。ここで、（ｐ１，ｑ１）と（ｐ２，ｑ２）の各組はそれぞれ互いに異なる大きな素数の組になっており、Ｎ１＝ｐ１×ｑ１，Ｎ２＝ｐ２×ｑ２である。また、$I = s^2 \pmod{N1}$，$PU \times SU = 1 \pmod{(p2-1)(q2-1)}$ が成立している。なお、ｐ１＝ｐ２，ｑ１＝ｑ２としてもよい。

【０１３４】さらに、各情報提供者ごとにｐ，ｑ，ＰＣ，ＳＣを設定し、このうちＮ，ＰＣを情報提供者の公開情報（公開鍵）として公開し、ＳＣを情報提供者の秘密情報（秘密鍵）として情報提供者秘密情報蓄積手段２０１に蓄積して情報提供者に秘密裏に配布する。ここで、ｐ，ｑは互いに異なる大きな素数であり、Ｎ＝ｐｑである。また、$PC \times SC = 1 \pmod{(p-1)(q-1)}$ が成立している。

【０１３５】（１）情報配送ステップ

情報提供者は、乱数発生手段２０９によりｇビットサイズの情報暗号化用秘密鍵W_i（ｉ＝１，２，…，ｇ）を生成して一時メモリ２０３に蓄積する（Ｓ２０１）。ここで、一般にｇの値は共通鍵暗号手段１０５，２０５で使用する秘密鍵の鍵長と等しいかそれ以上ある。なお、ここでは情報暗号化用秘密鍵W_i（ｉ＝１，２，…，ｇ）について乱数発生手段２０９により生成しているが、実際には関数を使用して生成したり、あるいは特定の秘密鍵を一意的に使用するなどしても構わない。

【０１３６】次に、利用者に配送する情報Ｍを情報データベース２０２から取り出し（Ｓ２０２）、情報暗号化用秘密鍵W_i（ｉ＝１，２，…，ｇ）を秘密鍵として共通鍵暗号手段２０５により暗号文Ｃ＝$E_{(M)}$に暗号化した後（Ｓ２０３）、利用者に暗号文Ｃを通信回線３０（および通信制御手段１００，２００）を介して送信する（Ｓ２０４）。

【０１３７】利用者は、暗号文Ｃを情報蓄積手段１０９に受信／蓄積した後、受信した旨を通信回線３０を介して情報提供者に通知する（Ｓ２０５）。

【０１３８】（２）配送確認ステップ

利用者は、乱数発生手段１０３によりｇ個の乱数R_i（ｉ＝１，２，…，ｇ）を生成し、一時メモリ１０２に蓄積した後（Ｓ２０６）、それぞれの乱数について演算手段１０４により初期応答文$X_i = R_i^2 \pmod{N1}$（ｉ＝１，２，…，ｇ）を計算し（Ｓ２０７）、情報提供者の公開鍵ＰＣを用いて公開鍵暗号手段１０７により暗号化初期応答文$CX_i = X_i^{PC} \pmod{N}$（ｉ＝１，２，…，ｇ）に暗号化して（Ｓ２０８）、通信回線３０を介して情報提供者に送信する（Ｓ２０９）。

【０１３９】情報提供者は、情報提供者秘密情報蓄積手段２０１に蓄積された秘密鍵ＳＣを用いて公開鍵暗号手段２１０により受信した暗号化初期応答文CX_iを初期応答文$X_i = CX_i^{SC} \pmod{N}$（ｉ＝１，２，…，ｇ）に復号した後、一時メモリ２０３に蓄積する（Ｓ２１０）。

【０１４０】次に、一時メモリ２０３に蓄積された情報暗号化用秘密鍵W_i（ｉ＝１，２，…，ｇ）を秘密鍵配送文V_iおよび検査文e_i（ｉ＝１，２，…，ｇ）として一時メモリ２０３に蓄積した後（Ｓ２１１）、利用者の公開鍵ＰＵを用いて公開鍵暗号手段２１０により暗号化検査文$Ce_i = (e_1 \| e_2 \| \cdots \| e_g)^{PU} \pmod{N2}$（ｉ＝１，２，…，｜Ｎ２｜）に暗号化して（Ｓ２１２）、通信回線３０を介して送信する（Ｓ２１３）。ここで、｜Ｎ２｜はＮ２のビット数を表す。

【０１４１】利用者は、利用者秘密情報蓄積手段１０１に蓄積された秘密鍵ＳＵを用いて公開鍵暗号手段１０７により受信した暗号化検査文Ce_i（ｉ＝１，２，…，ｇ）を検査文$e_i = (Ce_1 \| Ce_2 \| \cdots \| Ce_{|N2|})^{SU} \pmod{N2}$（ｉ＝１，２，…，ｇ）に復号した後、一時メモリ１０２に蓄積する（Ｓ２１４）。

【０１４２】次に、演算手段１０４において検査文e_iのそれぞれのビットｉに対し、一時メモリ１０２に蓄積された乱数R_iと利用者秘密情報蓄積手段１０１に蓄積された利用者の秘密情報ｓとから$e_i = 0$ならば$Y_i = R_i$を、$e_i = 1$ならば$Y_i = sR_i \pmod{N1}$を計算し（Ｓ２１５）、応答文Y_i（ｉ＝１，２，…，ｇ）として情報提供者に通信回線３０を介して送信する（Ｓ２１６）。

【０１４３】情報提供者は、受信した応答文Y_i（ｉ＝１，２，…，ｇ）を一時メモリ２０３に蓄積した（Ｓ２１７）後、検証手段２０６において利用者の公開情報Ｉおよび一時メモリ２０３に蓄積された初期応答文X_iと応答文Y_iと検査文e_iとからそれぞれのビットｉに対し、$e_i = 0$ならば検証式$Y_i^2 = X_i \pmod{N1}$を、$e_i = 1$ならば検証式$Y_i^2 = X_i \times I \pmod{N1}$を満たすかどうかを検証する（Ｓ２１８）。この検証に失敗した場合には利用者は不正であるとみなしてそれ以降の利用を禁止し（Ｓ２１９Ａ）、そうでなければ正常に終了する（Ｓ２１９Ｂ）。

【０１４４】（３）情報取り出しステップ

利用者は、一時メモリ１０２に蓄積された検査文e_i（ｉ＝１，２，…，ｇ）から演算手段１０４において秘密鍵配送文V_iおよび情報暗号化用秘密鍵W_i（ｉ＝１，２，…，ｇ）を取り出し、情報蓄積手段１０９に蓄積する（Ｓ２２０）。

【０１４５】最後に、情報蓄積手段１０９に蓄積された

情報暗号化用秘密鍵W_i（ｉ＝１，２，…，ｇ）を秘密鍵として、共通鍵暗号手段１０５により情報蓄積手段１０９に蓄積された暗号文Ｃを復号し（Ｓ２２１）、要求した情報Ｍ＝Ｄ$_v$（Ｃ）を情報出力／利用手段１０６より獲得することができる（Ｓ２２２）。

【０１４６】上記の情報配送方法を用いれば、情報Ｍは初めに暗号文Ｃに暗号化されて利用者に送信されるため、暗号文Ｃを利用者が受信した時点では情報Ｍを獲得されることはない。そして、ゼロ知識証明プロトコルが正常に終了した時点で、ゼロ知識証明プロトコルによる利用者認証が正常に行われたことのほかに、検査文e_i（ｉ＝１，２，…，ｇ）を利用者が正常に受信し、適切な処理を行っていることがわかる。

【０１４７】また、利用者は検査文e_i（ｉ＝１，２，…，ｇ）を正しく受信していれば情報暗号化用秘密鍵W_i（ｉ＝１，２，…，ｇ）を生成し、利用者が要求した情報の暗号文Ｃを復号して情報Ｍを獲得することができるため、検査文e_i（ｉ＝１，２，…，ｇ）を利用者が正常に受信したことと利用者が要求した情報を正常に受信したこととは同値となる。したがって、情報提供者は要求された情報を正確かつ確実に利用者に配送したことを確認できる。

【０１４８】なお、上記の説明において公開鍵暗号方法を利用して暗号化／復号を行っている部分については、共通鍵暗号方法を利用しても当然構わない。また、上記の説明ではFiat Shamir 法をもとに説明したが、本方法は拡張Fiat Shamir 法（太田－岡本「Fiat-Shamir 法の高次への拡張」、電子情報通信学会技術研究報告ＩＳＥＣ８８－１３）を始めとする、素因数分解困難性あるいは離散対数問題等の困難性に安全性の根拠を置く全てのゼロ知識対話証明プロトコルに応用が可能である。

【０１４９】次に、本発明の第６実施例について説明する。

【０１５０】図１５は本発明の第６の実施例における情報配送システムの構成を示すブロック図であり、システム構成は情報提供者（端末）２０の情報提供者秘密情報蓄積手段２０１が必要ないことを除き、第５実施例の構成と同様である。

【０１５１】以下、図１６のフローチャートにしたがって情報配送ステップ、配送確認ステップ、情報取り出しステップの動作手順を説明する。

【０１５２】まず、準備段階として、信頼できるセンタが各利用者ごとにｐ１，ｑ１，Ｉ，ｓ，ｐ２，ｑ２，ＰＵ，ＳＵを設定し、このうちＮ１，Ｎ２，Ｉ，ＰＵを利用者の公開情報（公開鍵）として公開し、ｓ，ＳＵを利用者の秘密情報（秘密鍵）として利用者秘密情報蓄積手段１０１に蓄積して利用者に秘密裏に配布する。ここで、（ｐ１，ｑ１）と（ｐ２，ｑ２）の各組はそれぞれ互いに異なる大きな素数の組になっており、Ｎ１＝ｐ１×ｑ１，Ｎ２＝ｐ２×ｑ２である。また、$I=s^2 \pmod{N1}$，$PU \times SU = 1 \pmod{(p2-1)(q2-1)}$が成立している。なお、ｐ１＝ｐ２，ｑ１＝ｑ２としてもよい。

【０１５３】（１）情報配送ステップ
第５実施例と同様である（Ｓ２３１～２３５）。
（２）配送確認ステップ
利用者は、乱数発生手段１０３により｜Ｎ２｜個の乱数R_i（ｉ＝１，２，…，｜Ｎ２｜）を生成し、一時メモリ１０２に蓄積した後（Ｓ２３６）、それぞれの乱数について演算手段１０４により初期応答文$X_i = R_i^2 \pmod{N1}$（ｉ＝１，２，…，｜Ｎ２｜）を計算し（Ｓ２３７）、通信回線３０を介して情報提供者に送信する。（Ｓ２３８）。ここで、｜Ｎ２｜はＮ２のビット数を表す。

【０１５４】情報提供者は、受信した初期応答文X_i（ｉ＝１，２，…，｜Ｎ２｜）を一時メモリ２０３に蓄積する（Ｓ２３９）。次に、一時メモリ２０３に蓄積された情報暗号化用秘密鍵W_iを秘密鍵配送文V_i（ｉ＝１，２，…，ｇ）として利用者の公開鍵ＰＵを用いて公開鍵暗号手段２１０により暗号化し、検査文$e_i = (V_1 \| V_2 \| \cdots \| V_g)^{PU} \pmod{N2}$（ｉ＝１，２，…，｜Ｎ２｜）を生成した後、一時メモリ２０３に蓄積する（Ｓ２４０）。その後、検査文e_i（ｉ＝１，２，…，｜Ｎ２｜）を通信回線３０を介して送信する（Ｓ２４１）。

【０１５５】利用者は、受信した検査文e_i（ｉ＝１，２，…，｜Ｎ２｜）を一時メモリ１０２に蓄積した（Ｓ２４２）後、演算手段１０４において検査文e_iのそれぞれのビットｉに対し、一時メモリ１０２に蓄積された乱数R_iと利用者秘密情報蓄積手段１０１に蓄積された利用者秘密情報ｓとからe_i＝０ならば$Y_i = R_i$を、e_i＝１ならば$Y_i = s R_i \pmod{N1}$を計算し（Ｓ２４３）、応答文Y_i（ｉ＝１，２，…，ｇ）として情報提供者に通信回線３０を介して送信する（Ｓ２４４）。

【０１５６】情報提供者は、受信した応答文Y_i（ｉ＝１，２，…，｜Ｎ２｜）を一時メモリ２０３に蓄積した（Ｓ２４５）後、検証手段２０６において利用者の公開情報Ｉおよび一時メモリ２０３に蓄積された初期応答文X_iと応答文Y_iと検査文e_iとからそれぞれのビットｉに対し、e_i＝０ならば検証式$Y_i^2 = X_i \pmod{N1}$を、e_i＝１ならば検証式$Y_i^2 = X_i \times I \pmod{N1}$を満たすかどうかを検証する（Ｓ２４６）。この検証に失敗した場合には利用者は不正であるとみなしてそれ以降の利用を禁止し（Ｓ２４７Ａ）、そうでなければ正常に終了する（Ｓ２４７Ｂ）。

【０１５７】（３）情報取り出しステップ
利用者は、一時メモリ１０２に蓄積された検査文e_i（ｉ＝１，２，…，｜Ｎ２｜）を利用者秘密情報蓄積手段１０１に蓄積された秘密鍵ＳＵを用いて公開鍵暗号

手段１０７により秘密鍵配送文V_i＝（$e_1 \| e_2 \| \cdots \| e_{|N2|}$）^{SU} (mod Ｎ２)　（ｉ＝１，２，…，ｇ）に復号した（Ｓ２４８）後、演算手段１０４において情報暗号化用秘密鍵W_i（ｉ＝１，２，…，ｇ）を取り出し、情報蓄積手段１０９に蓄積する（Ｓ２４９）。

【０１５８】最後に、情報蓄積手段１０９に蓄積された情報暗号化用秘密鍵W_i（ｉ＝１，２，…，ｇ）を秘密鍵として、共通鍵暗号手段１０５により情報蓄積手段１０９に蓄積された暗号文Ｃを復号し（Ｓ２５０）、要求した情報Ｍ＝D_w（Ｃ）を情報出力／利用手段１０６より獲得することができる（Ｓ２５１）。

【０１５９】上記の情報配送方法を用いれば、第５実施例と全く同等の効果が得られる。また第５実施例と比較して、一時メモリ等に蓄積しなければならない情報量のサイズは大きくなるが、処理速度の遅い公開鍵暗号方法を利用する回数が１回ですむため、処理時間の短縮化が期待できる。

【０１６０】なお、上記の説明において公開鍵暗号方法を利用して暗号化／復号を行っている部分については共通鍵暗号方法を利用しても当然構わない。また、上記の説明ではFiat Shamir 法をもとに説明したが、本方法は拡張Fiat Shamir 法（太田－岡本「Fiat-Shamir 法の高次への拡張」、電子情報通信学会技術研究報告ＩＳＥＣ８８－１３）を始めとする、素因数分解困難性あるいは離散対数問題等の困難性に安全性の根拠を置く全てのゼロ知識対話証明プロトコルに応用が可能である。

【０１６１】次に、本発明の第７実施例について説明する。

【０１６２】図１７は本発明の第７の実施例における情報配送システムの構成を示すブロック図であり、１０は利用者（端末）を示し、公開鍵暗号手段１０７が必要ないことを除いて１００から１０９までの構成手段は第６実施例と同様であり、１１０は情報配送要求文を作成する入力手段である。２０は情報提供者（端末）を示し、公開鍵暗号手段２１０が必要ないことを除いて２００から２０６までと２０９の構成手段は第６実施例と同様であり、２０８は後日、情報を利用者に配送した事実を証明する証拠としての通信履歴Ｈを記録管理する通信履歴ファイルである。３０は利用者と情報提供者とを通信で接続する通信回線を表す。４０は後日、情報提供者が通信履歴ファイル２０８に記録管理している通信履歴Ｈについて、中立的立場によりその通信履歴Ｈの正当性を判定する調停者（端末）を表し、４０２は調停者が必要な情報を一時的に蓄積する一時メモリ、４０１は必要な演算を行う演算手段、４０３は正当性の判定を依頼された通信履歴Ｈについてその正当性を検証する検証手段である。

【０１６３】以下、図１８のフローチャートにしたがって情報配送ステップ、配送確認ステップ、情報取り出しステップの動作手順を、また図１９のフローチャートにしたがって調停での動作手順を説明する。

【０１６４】まず、準備段階として、信頼できるセンタが各利用者ごとにｐ１，ｑ１，Ｉ，ｓを設定し、このうちＮ１とＩを利用者の公開情報として公開し、ｓを利用者の秘密情報として利用者秘密情報蓄積手段１０１に蓄積して利用者に秘密裏に配布する。ここで、ｐ１とｑ１は互いに異なる大きな素数を表し、Ｎ１＝ｐ１×ｑ１である。また、Ｉ＝s^2 (mod Ｎ１) が成立している。

【０１６５】（１）情報配送ステップ

利用者は、情報提供者に提供して欲しい情報について入力手段１１０から情報配送要求文ＲＳを作成し、一時メモリ１０２に蓄積した（Ｓ２６１）後、通信回線３０を介して情報提供者に送信する（Ｓ２６２）。ここで、情報配送要求文ＲＳは、例えば図２０に示すように要求日時、利用者識別番号、要求情報名、要求情報コード等から構成される。なお、図２０は情報配送要求文ＲＳの構成形態を表している。

【０１６６】ここでは情報配送要求文ＲＳを利用者より情報提供者に送信しているが、実際には要求情報コードのみを利用者が情報提供者に送信するなどして、情報提供者と利用者がそれぞれ独自に同じ情報配送要求文ＲＳを作成するようにしてもよい。

【０１６７】情報提供者は、乱数発生手段２０９により乱数文Ｚをランダムに生成し（Ｓ２６３）、情報配送要求文ＲＳと生成した乱数文Ｚとを一時メモリ２０３に蓄積した（Ｓ２６４）後、情報配送要求文ＲＳと乱数文Ｚとから演算手段２０４中の第一の一方向性ランダムハッシュ関数ｆ１によりｇビットサイズの情報暗号化用秘密鍵W_i＝ｆ１（ＲＳ，Ｚ）（ｉ＝１，２，…，ｇ）を生成して一時メモリ２０３に蓄積する（Ｓ２６５）。ここで、一般にｇの値は共通鍵暗号手段１０５，２０５で使用する秘密鍵の鍵長と等しいかそれ以上である。次に、情報配送要求文ＲＳ中の要求情報コードをもとに、そのコードに対応する情報Ｍを情報データベース２０２から取り出し（Ｓ２６６）、情報暗号化用秘密鍵W_i（ｉ＝１，２，…，ｇ）を秘密鍵として共通鍵暗号手段２０５により暗号文Ｃ＝E_w（Ｍ）に暗号化した（Ｓ２６７）後、利用者に暗号文Ｃを通信回線３０を介して送信する（Ｓ２６８）。

【０１６８】利用者は、暗号文Ｃを情報蓄積手段１０９に受信／蓄積した後、受信した旨を通信回線３０を介して情報提供者に通知する（Ｓ２６９）。

【０１６９】（２）配送確認ステップ

利用者は、乱数発生手段１０３によりｇ個の乱数R_i（ｉ＝１，２，…，ｇ）を生成した後一時メモリ１０２に蓄積し（Ｓ２７０）、それぞれの乱数について演算手段１０４により初期応答文X_i＝R_i^2 (mod Ｎ１)（ｉ＝１，２，…，ｇ）を計算した後一時メモリ１０２に蓄積し（Ｓ２７１）、初期応答文X_i（ｉ＝１，２，…，ｇ）を通信回線３０を介して情報提供者に送信する

（Ｓ２７２）。

【０１７０】情報提供者は、受信した初期応答文X_i（ｉ＝１，２，…，ｇ）を一時メモリ２０３に蓄積した（Ｓ２７３）後、一時メモリ２０３に蓄積された情報配送要求文ＲＳと初期応答文X_i（ｉ＝１，２，…，ｇ）とから演算手段２０４中の第二の一方向性ランダムハッシュ関数ｆ２によりｇビットサイズの鍵暗号化用秘密鍵K_i＝ｆ２（ＲＳ，（$X_1 \| X_2 \| \cdots \| X_g$））（ｉ＝１，２，…，ｇ）を生成し、一時メモリ２０３に蓄積する（Ｓ２７４）。なお、ｆ１とｆ２は同じ関数でも当然構わない。

【０１７１】次に、一時メモリ２０３に蓄積された情報暗号化用秘密鍵W_iと鍵暗号化用秘密鍵K_i（ｉ＝１，２，…，ｇ）とから演算手段２０４中の第三の関数ｆ３により秘密鍵配送文V_i（ｉ＝１，２，…，ｇ）を生成し、検査文e_i（ｉ＝１，２，…，ｇ）として一時メモリ２０３に蓄積した（Ｓ２７５）後、利用者に検査文e_i（ｉ＝１，２，…，ｇ）を通信回線３０を介して送信する（Ｓ２７６）。こ

【外１】

こで、第三の関数ｆ３には例えば$V_i = f3(W_i, K_i) = W_i \oplus K_i$（ｉ＝１，２，…，ｇ）がある。なお、⊕は排他的論理和を表す。

利用者は、受信した検査文e_i（ｉ＝１，２，…，ｇ）を一時メモリ１０２に蓄積した（Ｓ２７７）後、演算手段１０４において検査文e_iのそれぞれのビットｉに対し、一時メモリ１０２に蓄積された乱数R_iと利用者秘密情報蓄積手段１０１に蓄積された利用者の秘密情報ｓとからe_i＝０ならば$Y_i = R_i$を、e_i＝１ならば$Y_i = sR_i \pmod{N1}$を計算し（Ｓ２７８）、応答文Y_i（ｉ＝１，２，…，ｇ）として情報提供者に通信回線３０を介して送信する（Ｓ２７９）。

【０１７２】情報提供者は、受信した応答文Y_i（ｉ＝１，２，…，ｇ）を一時メモリ２０３に蓄積した（Ｓ２８０）後、検証手段２０６において利用者の公開情報Ｉおよび一時メモリ２０３に蓄積された初期応答文X_iと応答文Y_iと検査文e_iとからそれぞれのビットｉに対し、e_i＝０ならば検証式$Y_i^2 = X_i \pmod{N1}$を、e_i＝１ならば検証式$Y_i^2 = X_i \times I \pmod{N1}$を満たすかどうかを検証する（Ｓ２８１）。この検証に失敗した場合には利用者は不正であるとみなしてそれ以降の利用を禁止し（Ｓ２８２）、成功した場合には図２１に示すように、一時メモリ２０３に蓄積された情報配送要求文ＲＳ、乱数文Ｚ、検査文e_i、応答文Y_i（ｉ＝１，２，…，ｇ）を通信履歴Ｈとして通信履歴ファイル２０８に記録管理する（Ｓ２８３）。なお、図２１は通信履歴Ｈの構成形態を示している。

【０１７３】（３）情報取り出しステップ

利用者は、一時メモリ１０２に蓄積された情報配送要求文ＲＳと初期応答文X_i（ｉ＝１，２，…，ｇ）とから演算手段１０４中の第二の一方向性ランダムハッシュ関数ｆ２によりｇビットサイズの鍵暗号化用秘密鍵K_i＝ｆ２（ＲＳ，（$X_1 \| X_2 \| \cdots \| X_g$））（ｉ＝１，２，…，ｇ）を生成し、一時メモリ１０２に蓄積する（Ｓ２８４）。次に、一時メモリ１０２に蓄積された検査文e_i（ｉ＝１，２，…，ｇ）から秘密鍵配送文V_i（ｉ＝１，２，…，ｇ）を生成し、生成した秘密鍵配送文V_iと鍵暗号化用秘密鍵K_i（ｉ＝１，２，…，ｇ）とから演算手段１０４中の第三の関数ｆ３の逆関数ｆ３′により情報暗号化用秘密鍵W_i（ｉ＝１，２，…，ｇ）を取り出し、情報蓄積手段１０９に蓄積する（Ｓ２８

【外２】

５）。ここで、例えば第三の関数ｆ３の$V_i = f3(W_i, K_i) = W_i \oplus K_i$（ｉ＝１，２，…，ｇ）に対し、第三の逆関数ｆ３′は$W_i = f3'(V_i, K_i) = V_i \oplus K_i$（ｉ＝１，２，…，ｇ）となる。なお、⊕は排他的論理和を表す。

【０１７４】最後に、情報蓄積手段１０９に蓄積された情報暗号化用秘密鍵W_i（ｉ＝１，２，…，ｇ）を秘密鍵として共通鍵暗号手段１０５により情報蓄積手段１０９に蓄積された暗号文Ｃを復号し（Ｓ２８６）、要求した情報Ｍ＝Ｄ，（Ｃ）を情報出力／利用手段１０６より獲得することができる（Ｓ２８７）。

【０１７５】（４）調停

後日、利用者が要求した情報を受信していないと主張したり、情報配送の要求そのものを否定した場合には、情報提供者は通信履歴ファイル２０８に記録管理された通信履歴Ｈを提示し、調停者の一時メモリ４０２に蓄積する（Ｓ２９１）。

【０１７６】調停者は、演算手段４０１において利用者の公開情報Ｉと一時メモリ４０２に蓄積された通信履歴Ｈ中の検査文e_iおよび応答文Y_iからそれぞれのビットｉに対し、e_i＝０ならば、$X_i = Y_i^2 \pmod{N1}$をe_i＝１ならば$X_i = Y_i^2 / I \pmod{N1}$を計算し、一時メモリ４０２に蓄積する（Ｓ２９２）。

【０１７７】次に、一時メモリ４０２に蓄積された通信履歴Ｈ中の配送要求文ＲＳと乱数文Ｚとから演算手段４０１中の第一の一方向性ランダムハッシュ関数ｆ１によ

り情報暗号化用秘密鍵W_i＝ｆ１（ＲＳ，Ｚ）（ｉ＝１，２，…，ｇ）を（Ｓ２９３）、また情報配送要求文ＲＳと計算結果X_i（ｉ＝１，２，…，ｇ）とから演算手段４０１中の第二の一方向性ランダムハッシュ関数ｆ２により鍵暗号化用秘密鍵K_i＝ｆ２（ＲＳ，（$X_1 \| X_2 \| \cdots \| X_g$））（ｉ＝１，２，…，ｇ）をそれぞれ生成し、一時メモリ４０２に蓄積する（Ｓ２９４）。そして、情報暗号化用秘密鍵W_iと鍵暗号化用秘密鍵K_i（ｉ＝１，２，…，ｇ）とから演算手段４０１中の第三の関数ｆ３により秘密鍵配送文V_i（ｉ＝１，２，…，ｇ）を生成し（Ｓ２９５）、検査文e_i（ｉ＝１，２，…，ｇ）として検証手段４０３において一時メモリ４０２に蓄積された通信履歴Ｈ中の検査文e_i（ｉ＝１，２，…，ｇ）と一致するかどうかを検査する（Ｓ２９６）。一致すれば、通信履歴Ｈの正当性が証明されたことになり（Ｓ２９７）、利用者が情報配送を要求し、かつ要求した情報を受信していることが保証される。そうでなければ通信履歴Ｈは無効とされる（Ｓ２９８）。

【０１７８】上記の情報配送方式を用いれば、情報Ｍは初めに暗号文Ｃに暗号化されて利用者に送信されるため、暗号文Ｃを利用者が受信した時点では情報Ｍを獲得されることはない。そして、ゼロ知識証明プロトコルが正常に終了した時点で、ゼロ知識証明プロトコルによる利用者認証が正常に行われたことのほかに、検査文e_i（ｉ＝１，２，…，ｇ）を利用者が正常に受信したことの証明となる。

【０１７９】また、検査文e_i（ｉ＝１，２，…，ｇ）の他は利用者自身が作成した情報配送要求文ＲＳと初期応答文X_i（ｉ＝１，２，…，ｇ）とから情報暗号化用秘密鍵W_i（ｉ＝１，２，…，ｇ）を生成し、利用者が暗号文Ｃを復号して要求した情報Ｍを獲得することができるため、検査文e_i（ｉ＝１，２，…，ｇ）を利用者が正常に受信したことと利用者が要求した情報を正常に受信したこととは同値となる。したがって、情報提供者は正確かつ確実に情報を利用者に配送したことを確認できる。

【０１８０】また、上記の説明ではFiat Shamir 法をもとに説明したが、本方法は拡張FiatShamir 法（太田－岡本「Fiat-Shamir 法の高次への拡張」、電子情報通信学会技術研究報告ＩＳＥＣ８８－１３）を始めとする、素因数分解困難性あるいは離散対数問題等の困難性に安全性の根拠を置く全てのゼロ知識対話証明プロトコルに応用が可能である。

【０１８１】次に情報要求文ＲＳ、乱数文Ｚ、検査文e_i、応答文Y_i（ｉ＝１，２，…，ｇ）からなる通信履歴Ｈの関係では、ゼロ知識証明プロトコルにおける検証式と第一および第二の一方向性ランダムハッシュ関数とにより相互に関係し合っているため、一部を不正に改竄するなどして通信履歴Ｈを偽造することは不可能である。したがって、通信履歴Ｈを記録管理することにより、暗号文Ｃを復号して利用者が要求した情報Ｍを獲得できるための情報暗号化用秘密鍵W_i（ｉ＝１，２，…，ｇ）を利用者が確実に受信していることの証拠として、後日、調停者などの中立的な第三者に提示することができる。

【０１８２】以上の説明は、利用者が情報配送の要求を情報提供者に行い、情報提供者が要求された情報を正確かつ確実に利用者に配送したことを証明できるものであり、例えば情報Ｍを著作物などの有料情報とした場合、上記の情報配送方式によって情報提供者が利用者に情報Ｍを送信することにより、情報提供者が記録管理する通信履歴Ｈを著作権使用料等の情報料を徴収するときの証明情報として利用できるなど、様々な利用が可能である。

【０１８３】次に本発明の第８実施例について説明する。

【０１８４】図２２は本発明の第８実施例における情報配送システムの構成を示すブロック図であり、１０は利用者の端末（端末）を示し、１００から１０７までと１０９は第５の実施例と同様の構成であり、１１０は情報配送要求文を作成する入力手段、１０８は分割されたブロック情報を元の情報に再構成する情報再構成手段である。２０は情報提供者（端末）を示し、２００から２０６までと２０９と２１０は第５実施例と同様の構成であり、２０８は後日、情報を利用者に配送した事実を証明する証拠としての通信履歴Ｈを記録管理する通信履歴ファイル、２０７は情報を任意ビット長の複数のブロックに分割し、蓄積する情報分割手段である。３０は利用者と情報提供者とを通信で接続する通信回線を表す。４０は調停者（端末）を表し、４０１から４０３までは第７実施例と同様の構成であり、４０４は情報を任意ビット長の複数のブロックに分割し、蓄積する情報分割手段である。

【０１８５】以下、図２３および図２４のフローチャートにしたがって情報配送ステップ、配送確認ステップ、情報取り出しステップの動作手順を、また図２５のフローチャートにしたがって調停での動作手順を説明する。

【０１８６】まず、準備段階として、信頼できるセンタが各利用者ごとにｐ１，ｑ１，Ｉ，ｓを設定し、このうちＮ１とＩを利用者の公開情報として公開し、ｓを利用者の秘密情報として利用者秘密情報蓄積手段１０１に蓄積して利用者に秘密裏に配布する。ここで、ｐ１とｑ１は互いに異なる大きな素数を表し、Ｎ１＝ｐ１×ｑ１である。また、$I = s^2 \pmod{N1}$が成立している。

【０１８７】さらに、各情報提供者ごとにｐ，ｑ，ＰＣ，ＳＣを設定し、このうちＮ，ＰＣを情報提供者の公開情報（公開鍵）として公開し、ＳＣを情報提供者の秘密情報（秘密鍵）として情報提供者秘密情報蓄積手段２０１に蓄積して情報提供者に秘密裏に配布する。ここで、ｐ，ｑは互いに異なる大きな素数であり、Ｎ＝ｐｑ

である。また、ＰＣ×ＳＣ＝１（mod(p-1)(q-1)）が成立している。

【０１８８】（１）情報配送ステップ

利用者は、情報提供者に提供して欲しい情報入力について入力手段１１０から情報配送要求文ＲＳを作成し、一時メモリ１０２に蓄積した（Ｓ３０１）後、情報提供者の公開鍵ＰＣを用いて公開鍵暗号手段１０７により暗号化情報配送要求文ＣＲ＝RS^{PC}（mod Ｎ）に暗号化し（Ｓ３０２）、通信回線３０を介して情報提供者に送信する（Ｓ３０３）。ここで、情報配送要求文ＲＳは、第７実施例と同じように、例えば要求日時、利用者識別番号、要求情報名、要求情報コード等から構成される。

【０１８９】情報提供者は、情報提供者秘密情報蓄積手段２０１に蓄積された秘密鍵ＳＣを用いて、公開鍵暗号手段２１０により受信した暗号化情報配送要求文ＣＲを情報配送要求文$RS=CR^{SC}$（mod Ｎ）に復号した後一時メモリ２０３に蓄積し（Ｓ３０４）、また乱数発生手段２０９により乱数文Ｚをランダムに生成した後一時メモリ２０３に蓄積する（Ｓ３０５）。

【０１９０】次に、情報配送要求文ＲＳと乱数文Ｚとから演算手段２０４中の第一の一方向性ランダムハッシュ関数ｆ１によりｇビットサイズの情報暗号化用秘密鍵$W_i=f1(RS, Z)$（ｉ＝１，２，…，ｇ）を生成して一時メモリ２０３に蓄積する（Ｓ３０６）。ここで、一般にｇの値は共通鍵暗号手段１０５，２０５で使用する秘密鍵の鍵長と等しいかそれ以上である。その後、情報配送要求文ＲＳ中の要求情報コードをもとに、そのコードに対応する情報Ｍを情報データベース２０２から取り出し（Ｓ３０７）、情報暗号化用秘密鍵W_i（ｉ＝１，２，…，ｇ）を秘密鍵として共通鍵暗号手段２０５により暗号文$C=E_{\blacktriangledown}(M)$に暗号化した（Ｓ３０８）後、利用者に暗号文Ｃを通信回線３０を介して送信する（Ｓ３０９）。

【０１９１】利用者は、暗号文Ｃを情報蓄積手段１０９に受信／蓄積した後、受信した旨を通信回線３０を介して情報提供者に通知する（Ｓ３１０）。

【０１９２】（２）配送確認ステップ

情報提供者は、情報分割手段２０７において一時メモリ２０３に蓄積された情報暗号化用秘密鍵W_i（ｉ＝１，２，…，ｇ）を任意ビット長サイズの複数のブロックに分割し、情報暗号化用ブロック秘密鍵として蓄積する（Ｓ３１１）。ここでは説明を簡単にするため、分割したブロック数をｍ、全てのブロックについてビット長をＬで一定とし、分割した情報暗号化用秘密鍵を情報暗号化用ブロック秘密鍵WB_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｍ）と表す。すなわち、$WB_{ij}=W_{(i+L(j-1))}$であり、例えば$WB_{11}=W_1$、$WB_{L1}=W_L$、$WB_{12}=W_{L+1}$、$WB_{Lm}=W_g$のようになる。

【０１９３】これより以下の処理は第ｊブロックについてのものであり、配送確認ステップは第１ブロックから第ｍブロックまで各ブロックごとに以下の処理を順次（ｍ回）繰り返し行う。

【０１９４】まず利用者は、乱数発生手段１０３によりＬ個の乱数R_{ij}（ｉ＝１，２，…，Ｌ）を生成した後一時メモリ１０２に蓄積し（Ｓ３１２）、それぞれについて演算手段１０４により初期応答文$X_{ij}=R_{ij}^2$（mod Ｎ１）（ｉ＝１，２，…，Ｌ）を計算した後一時メモリ１０２に蓄積し（Ｓ３１３）、初期応答文X_{ij}（ｉ＝１，２，…，Ｌ）を通信回線３０を介して情報提供者に送信する（Ｓ３１４）。

【０１９５】情報提供者は、受信した初期応答文X_{ij}（ｉ＝１，２，…，Ｌ）を一時メモリ２０３に蓄積した（Ｓ３１５）後、一時メモリ２０３に蓄積された情報配送要求文ＲＳと初期応答文X_{ij}（ｉ＝１，２，…，Ｌ）とから演算手段２０４中の第二の一方向性ランダムハッシュ関数ｆ２によりＬビットサイズの鍵暗号化用秘密鍵$K_{ij}=f2(RS, (X_{1j} \| X_{2j} \| \cdots \| X_{Lj}))$（ｉ＝１，２，…，Ｌ）を生成して一時メモリ２０３に蓄積する（Ｓ３１６）。なお、ｆ１とｆ２は同じ関数でも当然構わない。

【０１９６】次に、情報分割手段２０７に蓄積された第ｊブロック目の情報暗号化用ブロック秘密鍵WB_{ij}（ｉ＝１，２，…，Ｌ）と一時メモリ２０３に蓄積された鍵暗号化用秘密鍵K_{ij}（ｉ＝１，２，…，Ｌ）とから演算手段２０４中の第三の関数ｆ３により秘密鍵配送文V_{ij}（ｉ＝１，２，…，Ｌ）を生成し、検査文e_{ij}（ｉ＝１，２，…，Ｌ）として一時メモリ２０３に蓄積した（３１７）後、利用者に検査文e_{ij}（ｉ＝１，２，…，Ｌ）を通信回線３０を介して送信する（Ｓ３１８）

【外３】

$$V_{ij}=f3(W_{ij}, K_{ij})=W_{ij}\oplus K_{ij}$$

。ここで、関数ｆ３には例えば（ｉ＝１，２，…，Ｌ）がある。なお、⊕は排他的論理和を表す。

利用者は、受信した検査文e_{ij}（ｉ＝１，２，…，Ｌ）を一時メモリ１０２に蓄積した（Ｓ３１９）後、演算手段１０４において検査文e_{ij}のそれぞれのビットｉに対し、一時メモリ１０２に蓄積された乱数R_{ij}と利用者秘密情報蓄積手段１０１に蓄積された利用者の秘密情報ｓとから、$e_{ij}=0$ならば$Y_{ij}=R_{ij}$を、$e_{ij}=1$ならば$Y_{ij}=sR_{ij}$（mod Ｎ１）を計算し（Ｓ３２０）、応答文Y_{ij}（ｉ＝１，２，…，Ｌ）として情報提供者に通信回線３０を介して送信する（Ｓ３２１）。

【０１９７】情報提供者は、受信した応答文Y_{ij}（ｉ＝１，２，…，Ｌ）を一時メモリ２０３に蓄積した（Ｓ３２２）後、検証手段２０６において利用者の公開情報Ｉおよび一時メモリ２０３に蓄積された初期応答文X_{ij}と応答文Y_{ij}と検査文e_{ij}とからそれぞれのビットｉに対

し、$e_{ij}=0$ならば検証式$Y_{ij}^{2}=X_{ij}$ (mod N1)を、$e_{ij}=1$ならば検証式$Y_{ij}^{2}=X_{ij}\times I$ (mod N1)を満たすかどうかを検証する（Ｓ３２３）。この検証に失敗した場合には利用者は不正であるとみなして、ただちにプロトコルの実行を中止し（Ｓ３２４）、成功した場合にはすべてのブロックが終了するまで以上の処理を繰り返す（Ｓ３２５）。そして、第１ブロックから第mブロックまでの全てのブロックについて検証に成功した場合には、一時メモリ２０３に蓄積された情報配送要求文ＲＳ、乱数文Ｚ、検査文e_{ij}、応答文Y_{ij}（ｉ＝１，２，…，Ｌ：ｉ＝１，２，…，ｍ）を通信履歴Ｈとして通信履歴ファイル２０８に記録管理する（Ｓ３２６）。

【０１９８】（３）情報取り出しステップ

利用者は、各ブロックについて一時メモリ１０２に蓄積された情報配送要求文ＲＳと初期応答文X_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｍ））とから演算手段１

$$=V_{ij}\oplus K_{ij}\ (i=1,\ 2,\ \cdots,\ L:\ j=1,\ 2,\ \cdots,\ m)$$

となる。なお、⊕は排他的論理和を表す。

【０２００】その後に、情報再構成手段１０８により蓄積された情報暗号化用ブロック秘密鍵WB_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｍ）を用いて情報暗号化用秘密鍵W_i（ｉ＝１，２，…，ｇ）に再構成して情報蓄積手段１０９に蓄積する（Ｓ３３０）。

【０２０１】最後に、情報蓄積手段１０９に蓄積された情報暗号化用秘密鍵W_i（ｉ＝１，２，…，ｇ）を秘密鍵として、共通暗号手段１０５により情報蓄積手段１０９に蓄積された暗号文Ｃを復号し（Ｓ３３１）、要求した情報Ｍ＝Ｄ。（Ｃ）を情報出力／利用手段１０６より獲得することができる（Ｓ３３２）

（４）調停

後日、利用者が要求した情報を受信していないと主張したり、情報配送の要求そのものを否定した場合には、情報提供者は通信履歴ファイル２０８に記録管理された通信履歴Ｈを提示し、調停者の一時メモリ４０２に蓄積する（Ｓ３４１）。

【０２０２】調停者は、演算手段４０１において利用者の公開情報Ｉと一時メモリ４０２に蓄積された通信履歴Ｈ中の検査文e_{ij}および応答文Y_{ij}からそれぞれのビットｉに対し、$e_{ij}=0$ならば、$X_{ij}=Y_{ij}^{2}$ (mod N1)を$e_{ij}=1$ならば$X_{ij}=Y_{ij}^{2}/I$ (mod N1)を計算し、一時メモリ４０２に蓄積する（Ｓ３４２）。次に、一時メモリ４０２に蓄積された通信履歴Ｈ中の情報配送要求文ＲＳと乱数文Ｚとから演算手段４０１中の第一の一方向性ランダムハッシュ関数ｆ１により情報暗号化用秘密鍵$W_i=f1$（ＲＳ，Ｚ）（ｉ＝１，２，…，ｇ）を生成した（Ｓ３４３）後、情報分割手段４０４において情報暗号化用ブロック秘密鍵WB_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｍ）に分割して蓄積する（Ｓ３４４）。

【０２０３】各ブロック（第ｊブロック）について、一時メモリ４０２に蓄積された情報配送要求文ＲＳと計算結果X_{ij}（ｉ＝１，２．…，Ｌ）とから演算手段４０１中の第二の一方向性ランダムハッシュ関数ｆ２により鍵暗号化用秘密鍵$K_{ij}=f2$（ＲＳ，$(X_{1j}\|X_{2j}\|\cdots\|X_{Lj})$）（ｉ＝１，２，…，Ｌ）を生成して一時メモリ４０２に蓄積する（Ｓ３４５）。そして、情報分割手段４０４に蓄積された情報暗号化用ブロック秘密鍵W_{ij}と一時メモリ４０２に蓄積された鍵暗号化用秘密鍵K_{ij}（ｉ＝１，２，…，Ｌ）とから演算手段４０１中の第三の関数ｆ３により秘密鍵配送文V_{ij}（ｉ＝１，２，…，Ｌ）を生成し（Ｓ３４６）、検査文e_{ij}（ｉ＝１，２，…，Ｌ）として検証手段４０３において一時メモリ４０２に蓄積された通信履歴Ｈ中の検査文e_{ij}（ｉ＝１，２，…，Ｌ）と一致するかどうかを検査する（Ｓ３４７）。全てのブロック（第１ブロックから第mブロックまでのmブロック）について一致すれば（Ｓ３４８）、通信履歴Ｈの正当性が証明されたことになり（Ｓ３４９）、利用者が情報配送を要求し、かつ要求した情報を受信していることが保証される。そうでなければ通信履歴Ｈは無効とされる（Ｓ３５０）。

【０２０４】上記の情報配送方式を用いれば、第７実施例と同様の効果が得られるほかに、情報提供者と利用者の間で情報配送要求文ＲＳについて暗号通信されているので、第三者が通信系列を盗聴したとしても、盗聴した通信系列からは情報配送要求文ＲＳおよび鍵暗号化用秘密鍵K_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｍ）を求めることができない。また、情報暗号化用秘密鍵W_i（ｉ＝１，２．…，ｇ）は検査文e_{ij}と鍵暗号化用秘密鍵K_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｍ）

【外４】

とから求められることから、情報暗号化用秘密鍵W_i（i＝1，2，…，g）を第三者が求めることができないことと同値となるので、第三者が暗号文Cを復号し、不正に情報Mを獲得することを防止することが可能となる。

【０２０５】さらに、情報提供者と利用者との間の通信が情報暗号化用秘密鍵W_i（i＝1，2，…，g）の分割ブロック数mと同じ回数だけ繰り返し行われるため、途中で情報提供者の検証に失敗した場合にはそれ以降の通信は打ち切られ、残りの検査文は送信されない。すなわち、利用者が知ることのできる検査文は検証に失敗する以前のもののみに限られるので、情報提供者の検証を失敗させた利用者は暗号文Cを復号するために必要な情報の一部しか獲得することができず、結果として正しい情報暗号化用秘密鍵W_i（i＝1，2，…，g）を生成することが不可能となる。

【０２０６】したがって、利用者の秘密情報sを知らない不正な利用者が不正な応答文Yij（i＝1，2，…，L：j＝1，2，…，m）を送信する場合はもとより、応答文そのものを送信しないような不正行為を行い、情報提供者が要求された情報Mを利用者に配送した事実を証明する通信履歴Hを情報提供者が記録管理できないにもかかわらず、利用者が要求した情報Mを獲得するのに必要な検査文e_{ij}（（i＝1，2，…，L：j＝1，2，…，m）を受信し、情報Mを不正に復号／獲得してしまうことがないようにすることが可能である。

【０２０７】また、上記の説明では分割するブロックを各ブロックともビット長をLで一定としたが、例えば第１ブロックは１ビット、第２ブロックは２ビット、第３ブロックは４ビットというようにブロックごとにビット長サイズを変えても当然構わない。

【０２０８】最後に、上記の説明における暗号通信のうち、公開鍵暗号方法による暗号通信については共通鍵暗号方法による暗号通信を行っても当然構わない。また、FiatShamir 法をもとに説明をしたが、本方法は拡張Fiat-Shamir 法（太田－岡本「Fiat-Shamir 法の高次への拡張」、電子情報通信学会技術研究報告ＩＳＥＣ８８－１３）を始めとする、素因数分解困難性あるいは離散対数問題等の困難性に安全性の根拠を置く全てのゼロ知識対話証明プロトコルに応用が可能である。

【０２０９】以上説明したとおり、本発明の第５～第８実施例によれば、ゼロ知識証明プロトコルを利用した情報配送方法では、第一に情報配送ステップにおいて、利用者が要求した情報は情報提供者によって暗号化されて利用者に配送されるため、この時点では要求した情報そのものを利用者が取り出すことはできない。第二に配送確認ステップで行われるプロトコル動作自体は利用者認証としてのゼロ知識証明プロトコルと同等であるため、ゼロ知識証明プロトコルと同じように不正な利用者が情報提供者の検証をクリアすることはほぼ不可能である。第三に配送確認ステップが正常に終了した場合には、ゼロ知識証明プロトコルが正常に終了したことと同値であるから、情報提供者は利用者が検査文を正しく受信し、適正な処理をしていると判断できる。第四に情報取り出しステップにおいて、利用者は検査文を正しく受信できれば、秘密鍵配送文及び情報暗号化用秘密鍵を作成することができるので、この時点で前記情報暗号化用秘密鍵により暗号化された情報を復号し、要求した情報を取り出すことができる。したがって、これらの効果により、情報配送方法の全てのステップが終了した場合には、情報提供者は正規の利用者に対して要求された情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送し、かつ確実に利用者が受信したことが確認できるので、情報提供者は利用者が要求した情報を利用者まで確実に配送したと判断できる。

【０２１０】又、本発明の第５、第６実施例によれば、検査文について暗号通信をすることは、情報暗号化用秘密鍵についても暗号通信をしていることと同等の効果が得られることになり、第三者が通信路を盗聴したとしてもこれらの秘密鍵が知られることはない。さらに、情報暗号化用秘密鍵を解読するために有効な情報も得られないようにすることもできる。

【０２１１】又、本発明の第７、第８実施例によれば、情報提供者にとって都合のよい情報暗号化用秘密鍵を不正に作成できないようにすることができる。

【０２１２】又、通信履歴を偽造することは不可能であるので、情報提供者は正規の利用者に対して要求された情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送し、かつ確実に利用者が受信したことを後日証明できる証拠能力を持つことができる。

【０２１３】又、証拠能力を有する通信履歴を必要に応じて提示できるようになる。また、情報提供者が情報を配送した事実の証拠として記録管理しなければならない情報量が桜井（特開平５－１２３２１）の方式と比較して大幅に削減できる。

【０２１４】又、情報提供者と利用者の間で情報の提供の有無について調停をする必要が生じた場合、裁判所等の中立な調停機関が証拠能力を有する通信履歴についてその正当性を検査することにより、情報提供者と利用者のどちらの主張が正当であるのかを判定できる。

【０２１５】又、本発明の第８実施例によれば、情報配送要求文を暗号送信することにより、第三者による情報配送要求文の盗聴を防止し、どんな情報を要求したかなどの利用者のプライバシーが保護できる。

【０２１６】又、鍵暗号化用秘密鍵及び情報暗号化用秘密鍵については、情報提供者と利用者のみの秘密の情報によりスクランブルされるので、第三者が通信路を盗聴したとしてもこれらの秘密鍵が知られることはなく、ま

た秘密鍵を解読するために有効な情報も得られない。したがって、利用者が要求した情報を第三者が不正に獲得することはできない。

【０２１７】又、例えば不正な利用者による利用などにより配送確認ステップの途中で情報提供者の検証に失敗した場合には、ただちにプロトコルの実行が中止され、検証に失敗した以降のブロックは利用者に送信されないことになる。したがって、情報提供者の検証を失敗させた利用者は暗号化された情報を復号するために必要な情報の一部しか獲得することができず、結果として鍵暗号化用秘密鍵もしくは情報暗号化用秘密鍵を生成することが不可能となるので、不正な利用者が要求した情報を不正に獲得してしまうことがないようにできる。

【０２１８】又、これらの実施例によれば、情報提供者が要求された情報を利用者に確実に配送し、かつ利用者が確実に受信していることを情報提供者が確認できるシステムとなる。また、必要に応じて情報提供者が利用者を認証する利用者認証方法としてのゼロ知識証明プロトコルを単独に使用することもできる。

【０２１９】又、情報暗号化秘密鍵を生成するときに乱数文を利用できるようにしたシステムとなる。

【０２２０】又、本発明の第５、第８実施例によれば、情報提供者が秘密に保持すべき情報を蓄積することができる情報提供者秘密情報蓄積手段を有したシステムとなる。

【０２２１】又、本発明の第５、第６、第８実施例によれば、情報提供者と利用者の間で公開鍵暗号方法による暗号通信ができるようにしたシステムとなる。

【０２２２】又、本発明の第７、第８実施例によれば、情報配送要求文を簡単に作成するための入力手段を利用者端末に備えたシステムとなる。

【０２２３】又、鍵暗号化用秘密鍵と秘密鍵配送文との生成機能を有し、情報暗号化用秘密鍵と鍵暗号用秘密鍵とを利用した情報配送ができるようにしたシステムとなる。

【０２２４】又、証拠能力を有する通信履歴を必要に応じて提示できるようにしたシステムとなる。

【０２２５】又、裁判所等の中立な調停機関により、証拠能力を有する通信履歴についてその正当性を検査し、情報提供者と利用者のどちらの主張が正当であるのかを判定することができるようにしたシステムとなる。

【０２２６】又、本発明の第８実施例によれば、不正な利用者があることを検出した際には直ちにプロトコルの実行を中止して、不正な利用者が要求した情報を不正に獲得してしまうことがないようにしたシステムとなる。

【０２２７】次に本発明の第９実施例について説明する。

【０２２８】図２６は本発明の第９実施例における情報配送システムの構成を示すブロック図であり、１０は情報の配送を受ける利用者（端末）を示し、１００は通信回線３０を制御する通信制御手段、１０１は利用者の秘密情報を蓄積しておく利用者秘密情報蓄積手段、１０５は共通鍵暗号方法（例えば、ＤＥＳ，ＦＥＡＬ）を利用する共通鍵暗号手段、１０７は公開鍵暗号方法（例えば、ＲＳＡ）を利用する公開鍵暗号手段、１０９は情報提供者からの配送された情報を蓄積する情報蓄積手段、１０２は利用者が必要な情報を一時的に蓄積する一時メモリ、１０３は利用者が乱数を生成するための乱数発生手段、１０４は必要な演算を行う演算手段、１０６は情報を出力もしくは利用する情報出力／利用手段である。２０は情報を提供する情報提供者（端末）を示し、２００は通信回線３０を制御する通信制御手段、２０１は情報提供者の秘密情報を蓄積しておく情報提供者秘密情報蓄積手段、２０５は共通鍵暗号方法を利用する共通鍵暗号手段、２１０は公開鍵暗号方法を利用する公開鍵暗号手段、２０２は提供する情報が蓄積してある情報データベース、２０３は情報提供者が必要な情報を一時的に蓄積する一時メモリ、２０４は必要な演算を行う演算手段、２０６は情報の正当性を検証する検証手段、２０８は後日情報を利用者に配送した事実を証明する証拠としての通信履歴データＨを記録管理する通信履歴ファイル、２０９は情報提供者が乱数を生成するための乱数発生手段である。３０は利用者として情報提供者とを通信で接続する通信回線を表す。４０は後日、情報提供者が通信履歴ファイル２０８に記録管理している通信履歴データＨについて、中立的立場によりその通信履歴データＨの正当性を判定する調停者（端末）を表し、４０２は調停者が必要な情報を一時的に蓄積する一時メモリ、４０５は公開鍵暗号方法を利用する公開鍵暗号手段、４０１は必要な演算を行う演算手段、４０３は正当性の判定を依頼された通信履歴データＨについてその正当性を検証する検証手段である。

【０２２９】以下、図２７および図２８のフローチャートにしたがって情報配送ステップ、配送確認ステップ、情報取り出しステップの動作手順を、また図２９のフローチャートにしたがって調停での動作手順を説明する。

【０２３０】なお、乱数Ｒと初期応答文Ｘと応答文Ｙを除くアルファベット文字は情報全体を表し、添え字付きアルファベット文字はその情報のビット情報を表す。例えば、情報暗号化用秘密鍵Ｗはｇビット長で構成される情報暗号化用秘密鍵全体のことを表し、情報暗号化用秘密鍵W_i（ｉ＝１，２，…，ｇ）は情報暗号化用秘密鍵の第ｉビット目のビット情報を表す。また、乱数Ｒと初期応答文Ｘと応答文Ｙの添え字は複数個生成される同一種類の情報の中のひとつの情報を表す。例えば、乱数R_i（ｉ＝１，２，…，ｇ）はｇ個生成される乱数の中の第ｉ番目に生成された乱数情報であることを表す。

【０２３１】（０）準備段階

信頼できるセンタが各利用者ごとにｐ１，ｑ１，ＩＤ，Ｓ，ｐ２，ｑ２，ＰＵ，ＳＵを設定し、このうちＮ１，

Ｎ２，ＩＤ，ＰＵを利用者の公開情報として公開し、Ｓ，ＳＵを利用者の秘密情報として利用者秘密情報蓄積手段１０１に蓄積して利用者に秘密裏に配布する。ここで、（ｐ１，ｑ１）と（ｐ２，ｑ２）の各組はそれぞれ互いに異なる大きな素数の組になっており、Ｎ１＝ｐ１×ｑ１，Ｎ２＝ｐ２×ｑ２である。また、ＩＤ＝Ｓ^{2} (mod Ｎ１)、ＰＵ×ＳＵ＝１ (mod(p2-1)(q2-1))が成立している。なお、ｐ１＝ｐ２，ｑ１＝ｑ２としてもよい。

【０２３２】さらに、各情報提供者ごとにｐ，ｑ，ＰＣ，ＳＣを設定し、このうちＮ，ＰＣを情報提供者の公開鍵として公開し、ＳＣを情報提供者の秘密鍵として情報提供者秘密情報蓄積手段２０１に蓄積して情報提供者に秘密裏に配布する。ここで、ｐ，ｑは互いに異なる大きな素数であり、Ｎ＝ｐｑである。またＰＣ×ＳＣ＝１ (mod (p-1)(q-1)) が成立している。

【０２３３】（１）情報配送ステップ

情報提供者は、乱数発生手段２０９でｇビット長の情報暗号化用秘密鍵Ｗを任意に生成して一時メモリ２０３に蓄積する（Ｓ３６１）。ここで、一般にｇの値は共通鍵暗号手段１０５と２０５で使用する秘密鍵の鍵長と等しいかそれ以上である。後に、情報Ｍを情報データベース２０２から取り出し（Ｓ３６２）、情報暗号化用秘密鍵Ｗを秘密鍵として共通鍵暗号手段２０５により暗号文Ｃ＝E_{W}(Ｍ)に暗号化した（Ｓ３６３）後、利用者に暗号文Ｃを通信回線３０を介して送信するる（Ｓ３６４）。

【０２３４】利用者は、暗号文Ｃを情報蓄積手段１０９に受信／蓄積した後、受信した旨を通信回線３０を介して情報提供者に通知する（Ｓ３６５）。

【０２３５】なお、ここではＳ３６４の暗号文Ｃの送信について通信回線３０を使用しているが、もちろんＣＤ－ＲＯＭなどの物理媒体に記録して、通信回線を使用せずに一般に配布するようにしても構わない。その場合には、Ｓ３６５の動作は省略されることが多い。

【０２３６】（２）配送確認ステップ

情報提供者は、公開鍵暗号手段２１０により情報暗号化用秘密鍵Ｗを情報提供者の公開鍵ＰＣで暗号化し（Ｓ３６６）、暗号化した情報暗号化用秘密鍵ＣＷ＝W^{PC} (mod Ｎ) を利用者に通信回線３０を介して通信する（Ｓ３６７）。

【０２３７】利用者は、公開鍵暗号手段１０７により利用者の秘密情報ＳＵを用いて暗号化された情報暗号化用秘密鍵ＣＷにディジタル署名を行い（Ｓ３６８）、署名付き情報暗号化用秘密鍵ＳＷ＝CW^{SU} (mod Ｎ２) を通信回線３０を介して情報提供者に送信する（Ｓ３６９）。

【０２３８】情報提供者は、署名付き情報暗号化用秘密鍵ＳＷを一時メモリ２０３に蓄積した（Ｓ３７０）後、検証手段２０６において利用者の公開鍵ＰＵを用いて署名検証式ＣＷ＝SW^{PU} (mod Ｎ２) を満たすうかどうかを検証する（Ｓ３７１）。この検証に失敗した場合には利用者は不正であると見做してただちにプロトコルの実行を中止する（Ｓ３７２）。また検証に成功した場合には、演算手段２０４において情報暗号化用秘密鍵Ｗを任意ビット長の複数のブロックに分割し、情報暗号化用ブロック秘密鍵ＷＢを生成する（Ｓ３７３）。ここでは説明を簡単にするため、分割したブロック数をｂ、全てのブロックについてビット長をＬで一定とし、分割した情報暗号化用秘密鍵を情報暗号化用ブロック秘密鍵WB_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）と表す。すなわち、$WB_{ij}=W_{(i+L(j-1))}$であり、例えば$WB_{11}=W_{1}$，$W_{L1}=W_{L}$，$WB_{12}=W_{L+1}$，$WB_{Lb}=W_{g}$のようになる。

【０２３９】利用者は、乱数発生手段１０３によりｇ個の乱数R_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）を生成した後一時メモリ１０２に蓄積し（Ｓ３７４）、それぞれについて演算手段１０４により初期応答文$X_{ij}=R_{ij}^{2}$ (mod Ｎ１)（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）を計算した後一時メモリ１０２に蓄積し（Ｓ３７５）、初期応答文X_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）を通信回線３０を介して情報提供者に送信する（Ｓ３７６）。

【０２４０】情報提供者は、初期応答文X_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）を一時メモリ２０３に蓄積した（Ｓ３７７）後、演算手段２０４中の一方向性ランダムハッシュ関数ｈ（・）によりｇビット長の鍵暗号化用秘密鍵$K_{ij}=h(X_{1j}\|X_{2j}\|\cdots\|X_{Lj})$（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）を生成し（Ｓ３７８）、情報暗号化用ブロック秘密鍵WB_{ij}と鍵暗号化用秘密鍵K_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）とから演算手段２０４中の関数ｆ（・）により検査文e_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）を生成して一時メモリ２０３に蓄積する（Ｓ３７９）。ここで、関数ｆには例えば$e_{ij}=f(W_{ij}, K_{ij})\oplus K_{ij}$（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）がある。

【外５】

なお、⊕は排他的論理和を表す。

これより以下の処理は第ｊブロックについてのものであり、配送確認ステップは第１ブロックから第ｂブロックまで各ブロックごとに以下の処理を順次（ｂ回）繰り返し行なう。

【０２４１】情報提供者は、利用者に検査文e_{ij}（ｉ＝１，２，…，Ｌ）を通信回線３０を介して送信する（Ｓ３８０）。

【０２４２】利用者は、検査文e_{ij}（ｉ＝１，２，…，

Ｌ）を一時メモリ１０２に蓄積した（Ｓ３８１）後、演算手段１０４において検査文e_{ij}のそれぞれのビットｉに対し、乱数R_{ij}と利用者の秘密情報Ｓとから、e_{ij}＝０ならば$Y_{ji}=R_{ij}$を、e_{ij}＝１ならば$Y_{ij}=S\times R_{ij}$（mod Ｎ１）を計算し（Ｓ３８２）、応答文Y_{ij}（ｉ＝１，２，…，Ｌ）として情報提供者に通信回線３０を介して送信する（Ｓ３８３）。

【０２４３】情報提供者は、応答文Y_{ij}（ｉ＝１，２，…，Ｌ）を一時メモリ２０３に蓄積した（Ｓ３８４）後、検証手段２０６において利用者の公開情報ＩＤ、初期応答文X_{ij}、応答文Y_{ij}および検査文e_{ij}とからそれぞれのビットｉに対し、e_{ij}＝０ならば検証式$Y_{ij}^{2}=X_{ij}$（mod Ｎ１）を、e_{ij}＝１ならば検証式$Y_{ij}^{2}=X_{ij}\times ID$（mod Ｎ１）を満たすかどうかを検証する（Ｓ３８５）。この検証に失敗した場合には利用者は不正であると見做して直ちにプロトコルの実行を中止し（Ｓ３８６）、また成功した場合にはＳ３８０に戻り、すべてのブロックが終了するまで以上の処理を繰り返す（Ｓ３８７）。そして、第１ブロックから第ｂブロックまでの全てのブロックについて検証に成功した場合には、情報暗号化用秘密鍵Ｗ、署名付き情報暗号化用秘密鍵ＳＷ、検査文e_{ij}、応答文Y_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）を通信履歴データＨとして通信履歴ファイル２０８に記録管理する（Ｓ３８８）。

【０２４４】（３）情報取り出しステップ

利用者は、初期応答文X_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）から演算手段１０４中の一方向性ランダムハッシュ関数ｈ（・）によりｇビット長の鍵暗号化用秘密鍵$K_{ij}=h(X_{1j}\|X_{2j}\|\cdots\|X_{Lj})$（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）を生成し（Ｓ３８９）、検査文e_{ij}と鍵暗号化用秘密鍵K_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）とから演算手段１０４中の関数ｆ（・）の逆関数ｆ′（・）により情報暗号化用ブロック秘密鍵WB_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）を取り出す（Ｓ３９０）。ここで、例えば関

【外６】

$$\text{数}f(\cdot)\text{の}e_{ij}=f(W_{ij},K_{ij})=W_{ij}\oplus K_{ij}(i=1,2,\cdots,L:j=1,2,\cdots,b)\text{に対し、逆関数}f'(\cdot)\text{は}W_{ij}=f'(e_{ij},K_{ij})=e_{ij}\oplus K_{ij}(i=1,2,\cdots,L:j=1,2,\cdots,b)\text{となる。なお、}\oplus\text{は排他的}$$

論理和を表す。その後、演算手段１０４に情報暗号化用ブロック秘密鍵WB_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）を用いて情報暗号化用秘密鍵W_{i}（ｉ＝１，２，…，ｇ）を生成し、情報蓄積手段１０９に蓄積する（Ｓ３９１）。最後に、情報暗号化用秘密鍵Ｗを秘密鍵として共通暗号手段１０５により情報蓄積手段１０９に蓄積された暗号文Ｃを復号し（Ｓ３９２）、情報Ｍ＝D_{v}（Ｃ）を情報出力／利用手段１０６より獲得することができる（Ｓ３９３）。

【０２４５】（４）調停

後日、利用者が情報を受信していないと主張した場合には、情報提供者は通信履歴ファイル２０８に記録管理された通信履歴データＨを提示し、調停者の一時メモリ４０２に蓄積する（Ｓ４０１）。

【０２４６】調停者は、公開暗号手段４０５において情報暗号化用秘密鍵Ｗを情報提供者の公開鍵ＰＣで暗号化した情報暗号化用秘密鍵$CW=W^{PC}$（mod Ｎ）を生成し（Ｓ４０２）、検証手段４０３において署名付き情報暗号化用秘密鍵ＳＷが利用者の公開鍵ＰＵを用いて署名検証式$CW=SW^{PU}$（mod Ｎ２）を満たすかどうかを検証する。（Ｓ４０３）。検証が失敗した時は通信履歴データＨは無効とされる（Ｓ４０４）。

【０２４７】署名の検証が成功した場合には、演算手段４０１において利用者の公開情報ＩＤと通信履歴データＨ中の検査文e_{ij}および応答文Y_{ij}からそれぞれのビットｉに対し、e_{ij}＝０ならば、$X_{ij}=Y_{ij}^{2}$（mod Ｎ１）を、e_{ij}＝１ならば$X_{ij}=Y_{ij}^{2}/ID$（mod Ｎ１）を計算して一時メモリ４０２に蓄積し（Ｓ４０５）、情報暗号化用秘密鍵Ｗから演算手段４０１において情報暗号化用ブロック秘密鍵WB_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）を生成する（Ｓ４０６）。次に、計算結果X_{ij}（ｉ＝１，２，…，Ｌ）から演算手段４０１中の一方向性ランダムハッシュ関数ｈ（・）によりｇビット長の鍵暗号化用秘密鍵$K_{ij}=h(X_{1j}\|X_{2j}\|\cdots\|X_{Lj})$（ｉ＝１，２，…，Ｌ；ｊ＝１，２，…，ｂ）を生成し（Ｓ４０７）、情報暗号化用ブロック秘密鍵WB_{ij}と鍵暗号化用秘密鍵K_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）とから演算手段４０１中の関数ｆ（・）により検査文e_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）を生成して（Ｓ４０８）、検証手段４０３において一時メモリ４０２に蓄積された通信履歴データＨ中の検査文e_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）と全てのビットについて一致するかどうかを検査する（Ｓ４０９）。全てのビットについて一致すれば、通信履歴データＨの正当性が証明されたことになり、利用者が情報Ｍを受信していることが保証される（Ｓ４１０）。そうでなければ通信履歴データＨは無効とされる（Ｓ４１１）。

【０２４８】上記の情報配送方式を用いれば、情報Ｍは初めに暗号文Ｃに暗号化されて利用者に送信もしくは物

理媒体により配布されるため、暗号文Ｃを利用者が入手した時点では情報Ｍを獲得されることはない。そしてプロトコルが正常に終了した時点で、ゼロ知識証明プロトコルによる利用者認証が正常に行なわれたことのほかに、検査文ｅを利用者が正常に受信したことが確認できる。また、検査文ｅの他は利用者自身が作成した初期応答文X_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）から情報暗号化用秘密鍵Ｗを生成し、利用者が暗号文Ｃを復号して情報Ｍを獲得することができるため、検査文ｅを利用者が正常に受信したことと利用者が情報Ｍを正常に受信したこととは同値となる。したがって、情報提供者は正確かつ確実に情報Ｍを利用者に配送したことを確認できる。

【０２４９】また、情報提供者と利用者との間の通信は情報暗号化用秘密鍵Ｗの分割ブロック数ｂと同じ回数だけ繰り返し行なわれるため、途中で情報提供者の検証に失敗した場合にはそれ以降の通信は打ち切られ、残りの検査文は送信されない。すなわち、利用者が知ることのできる検査文は検証に失敗する以前のもののみに限られるので、情報提供者の検証を失敗させた利用者は暗号文Ｃを復号するために必要な情報の一部しか獲得することができず、結果として正しい情報暗号化用秘密鍵Ｗを生成することが不可能となる。したがって、利用者の秘密情報Ｓを知らない不正な利用者が不正な応答文を送信する場合はもとより、応答文そのものを送信しないような不正行為を行ない、情報提供者が情報Ｍを利用者に配送した事実を証明する通信履歴データＨを情報提供者が記録できないにも関わらず、利用者が情報Ｍを獲得するのに必要な検査文ｅを全て受信し、情報Ｍを不正に復号／獲得してしまうことがないようにすることが可能である。なお、上記の説明では分割するブロックを各ブロックともビット長をＬで一定としたが、例えば第１ブロックは１ビット、第ブロックは２ビット、第３ブロックは４ビットというようにブロックごとにビット長を変えても当然構わない。

【０２５０】次に、署名付き情報暗号化用秘密鍵ＳＷは利用者にしか作成できないため、情報暗号化秘密鍵Ｗもしくは署名付き情報暗号化用秘密鍵ＳＷを情報提供者が不正に改変することはできない。また、情報暗号化用秘密鍵Ｗと、初期応答文X_{ij}、検査文e_{ij}、応答文Y_{ij}（ｉ＝１，２，…，Ｌ：ｊ＝１，２，…，ｂ）からなる通信系列との関係では、ゼロ知識証明プロトコルにおける検証式と一方向性ランダムハッシュ関数ｈ（・）とにより相互に関係し合っているため、それらの一部を不正に改竄するなどして通信系列を改変・偽造することは不可能である。したがって、通信履歴データＨを記録保管することにより暗号文Ｃを復号して利用者が情報Ｍを獲得できるための情報暗号化用秘密鍵Ｗを利用者が確実に受信していることの証拠として後に調停者などの中立的な第三者に提示することができる。

【０２５１】以上の説明は、情報提供者が情報Ｍを正確かつ確実に利用者に配送したことを証明できるものであり、例えば情報Ｍを著作物などの有料情報とした場合、上記の情報配送方法によって情報提供者が利用者に情報Ｍを送信することにより、情報提供者が記録管理する通信履歴データＨを著作権使用料等の情報料を徴収するときの証明情報として利用できるなど、様々な利用が可能である。

【０２５２】また、上記の説明ではFiat Shamir 法をもとに説明をしたが、本方法は拡張Fiat Shamir 法（太田－岡本「Fiat-Shamir 法の高次への拡張」、電子情報通信学会技術研究報告ＩＳＥＣ８８－１３）を始めとする、素因数分解困難性あるいは離散対数問題等の困難性に安全性の根拠を置く全てのゼロ知識対話証明プロトコルに応用が可能である。

【０２５３】以上説明したとおり、本発明の第９実施例によれば、ゼロ知識証明プロトコルを利用した情報配送方法では、第一に情報配送ステップにおいて、利用者が要求した情報は情報提供者によって暗号化されて利用者に配送されるため、この時点では要求した情報そのものを利用者が取り出すことはできない。第二に配送確認ステップで行われるプロトコル動作自体は利用者認証としてのゼロ知識証明プロトコルと同等であるため、ゼロ知識証明プロトコルと同じように不正な利用者が情報提供者の検証をクリアすることはほぼ不可能である。第三に配送確認ステップが正常に終了した場合には、ゼロ知識証明プロトコルが正常に終了したことと同値であるから、情報提供者は利用者が検査文を正しく受信し、適正な処理をしていると判断できる。第四に情報取り出しステップにおいて、利用者は検査文を正しく受信できれば情報暗号化用秘密鍵を作成することができるので、この時点で前記情報暗号化用秘密鍵により暗号化された情報を復号し、要求した情報を取り出すことができる。したがって、これらの効果により、情報配送方法の全てのステップが終了した場合には、情報提供者は正規の利用者に対して要求された情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送し、かつ確実に利用者が受信したことが確認できるので、情報提供者は利用者が要求した情報を利用者まで確実に配送したと判断できる。

【０２５４】又、情報提供者が自分に都合のよい情報暗号化用秘密鍵に不正に改竄できないようにすることができる。さらに、暗号化された情報暗号化用秘密鍵は情報提供者以外は復号することができないので、署名を行う時点では利用者に情報暗号化用秘密鍵を知られることはない。

【０２５５】又、通信履歴を偽造することは不可能であるので、情報提供者は正規の利用者に対して要求された情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送

し、かつ確実に利用者が受信したことを後日証明できる証拠能力を持つことができる。

【０２５６】又、証拠能力を有する通信履歴を必要に応じて提示できるようになる。また、情報提供者が情報を配送した事実の証拠として記録管理しなければならない情報量が桜井（特開平５－１２３２１）の方式と比較して大幅に削減できる。

【０２５７】又、情報提供者と利用者の間で情報の提供の有無について調停をする必要が生じた場合、裁判所等の中立な調停機関が証拠能力を有する通信履歴についてその正当性を検査することにより、情報提供者と利用者のどちらの主張が正当であるのかを判定できる。

【０２５８】又、例えば不正な利用者による利用などにより配送確認ステップの途中で情報提供者の検証に失敗した場合には、ただちにプロトコルの実行が中止され、検証に失敗した以降のブロックは利用者に送信されないことになる。したがって、情報提供者の検証を失敗させた利用者は暗号化された情報を復号するために必要な情報の一部しか獲得することができず、結果として情報暗号化用秘密鍵を生成することが不可能となるので、不正な利用者が要求した情報を不正に獲得してしまうことがないようにできる。

【０２５９】又、この実施例によれば、情報提供者が要求された情報を利用者に確実に配送し、かつ利用者が確実に受信していることを情報提供者が確認できるシステムとなる。また、必要に応じて情報提供者が利用者を認証する利用者認証方法としてのゼロ知識証明プロトコルを単独に使用することもできる。

【０２６０】又、情報暗号化秘密鍵を生成するときに乱数文を利用できるようにしたシステムとなる。

【０２６１】又、情報提供者が秘密に保持すべき情報を蓄積することができる情報提供者秘密情報蓄積手段を有したシステムとなる。

【０２６２】又、情報提供者と利用者の間で公開鍵暗号方法による暗号通信ができるようにしたシステムとなる。

【０２６３】又、鍵暗号化用秘密鍵と生成機能を有し、情報暗号化用秘密鍵と鍵暗号用秘密鍵とを利用した情報配送ができるようにしたシステムとなる。

【０２６４】又、証拠能力を有する通信履歴を必要に応じて提示できるようにしたシステムとなる。

【０２６５】又、裁判所等の中立な調停機関により、証拠能力を有する通信履歴についてその正当性を検査し、情報提供者と利用者のどちらの主張が正当であるのかを判定することができるようにしたシステムとなる。

【０２６６】又、不正な利用者があることを検出した際には直ちにプロトコルの実行を中止して、不正な利用者が要求した情報を不正に獲得してしまうことがないようにしたシステムとなる。

【０２６７】尚、本発明は上述した各実施例に限定されるものではなく、その要旨を逸脱しない範囲で、種々変形して実施することができる。

【０２６８】

【発明の効果】以上説明したとおり、上記第１実施例では、第一に情報提供者による利用者の認証方法としてゼロ知識証明プロトコルを利用しているため、ゼロ知識証明プロトコルの目的や従来からの利用方法からいっても、利用者が正当なカードを利用していなければ情報提供者の検証をクリアし続けることはほとんど不可能であり、認証段階でほぼ完全に拒絶される。

【０２６９】第二に情報提供者から配送情報を利用者へ配送する部分では、配送情報をゼロ知識証明プロトコルの検査文に含めて配送を行なっているため、ゼロ知識証明プロトコルが正常に終了すれば、カード上において間違いなく検査文、すなわち配送情報を受信・記録し、適正な処理をしていたことになる。また、途中で情報提供者の検証に失敗した場合にはそれ以降の認証は打ち切られ、残りの検査文は配送されないため、利用者が知ることのできる配送情報は検証に失敗する以前のものに限られる。

【０２７０】第三に通信履歴（前記X_i、前記Y_i、前記検査文e_{ji}）を記録管理することにより情報提供者と利用者との間で正常な認証が行なわれたことを情報提供者は確認できるので、第二の効果と合わせて利用者は配送情報を受信し、かつカードの蓄積手段１４に配送情報が記録されているはずである。このことは、情報提供者から開示される通信履歴と利用者から提出されるカードに記録された配送情報とを照合することによって、利用者が情報暗号化用秘密鍵Ｗを生成できる状態であるかどうかを判定できる。なお、この場合、利用者からカードの提出がない場合には、情報暗号化用秘密鍵Ｗは生成できる状態にあると判定する。

【０２７１】したがって、不正な利用者がシステムを利用したり、あるいは配送情報のすべてを不正に搾取したりすることはできない。また、正常に認証が終了しているにも関わらず利用者が配送情報を受信していないなどという不当な主張に対して、情報提供者は通信履歴を開示するとともに、利用者にカードを提出するよう要求することにより対抗できる。

【０２７２】また、上記第１実施例において、配送情報すべてを分割して検査文e_{ji}を生成する必要性はなく、例えば、配送情報の始めからｇｎビット目までを検査文e_{ji}（ｊ＝１，…，ｎ）とし、ｎ組の検査文e_{ji}によるゼロ知識証明プロトコルが終了した後、配送情報の残りの部分を一括して送信するような情報の配送方法とすれば、ｎの値を様々に変えることにより、ゼロ知識証明におけるセキュリティレベルを変えられるうえ、通信量を削減できる。例えばｎをL_s／ｇの半分とすれば、通信量もほぼ半分となる。

【０２７３】また、検査文e_{ji}の生成方法についても、

単純に配送情報を分割して生成するだけでなく、ダミー情報を付加したり、あるいは暗号化を行ったりして生成することも可能である。この場合、カード内にあらかじめ設定されている秘密情報、もしくは蓄積された検査文e_{ji}から自律的にダミー情報を除去、あるいは復号を行ったりして元の配送情報に復元する機能を持たせることにより、ゼロ知識証明を正常に終了しないかぎり、前記配送情報を取り出せないようにできる。したがって、第三者もしくは利用者が検査文e_{ji}を不正に搾取したり、大部分の検査文e_{ji}を受信した後、故意に認証を失敗させ、検査文e_{ji}のうち配送されてこない残りの部分を予測したりする等の不正行為を行ない、情報提供者が配送に失敗したと判断あるいは気がつかないうちに、第三者もしくは利用者が配送情報を獲得してしまうことがないようにできる。

【０２７４】また、上記第１実施例による情報配送方法およびシステムでは、ゼロ知識証明プロトコルに必要な情報はすべて耐タンパー装置上に組み込まれており、実際の情報配送においても耐タンパー装置上に組み込まれた手段のみを用いて実行されるため、前記情報が外部に漏れることはなく、たとえカード所有者であっても前記情報を知ることができない。したがって、カード自体を偽造したり、あるいはカード上の記録情報を書き変えたりする等の不正行為を防止できる。

【０２７５】一方、上記第２～第４実施例のゼロ知識証明プロトコルを利用した情報配送方法では、第一にプロトコルの動作自体は利用者認証としてのゼロ知識証明プロトコルと同等であるため、ゼロ知識証明プロトコルと同様に、不正な利用者が情報提供者の検証をクリアすることはほぼ不可能である。第二に配送確認ステップが正常に終了した場合には、ゼロ知識証明プロトコルが正常に終了したことと同値であるので、情報提供者は正しい利用者が情報を正しく受信していると判断できる。

【０２７６】又、情報を暗号化し暗号文として送信することにより、第三者による情報の盗聴を防止し、かつ第三者が情報を解読するために有効な情報も得られないようにすることもできる。

【０２７７】又、上記第２実施例によれば、暗号文の復号処理を配送確認ステップと切り離して実行することができる。

【０２７８】又、上記第２、第３実施例によれば、例えばハッシュ関数などを用いて情報（または利用者が復号可能な暗号文）から検査文を生成することにより検査文のサイズを小さくすることができ、配送確認ステップにおける通信量及び処理時間を削減できる。

【０２７９】又、上記第３実施例によれば、一方向性関数を用いて検査文を生成することにより、情報（または利用者が復号可能な暗号文）、応答文、及び検査文とからなる通信履歴の偽造を不可能にする。

【０２８０】又、例えば不正な利用者による利用などにより配送確認ステップの途中で情報提供者のプロトコルに失敗した場合には、直ちにプロトコルの実行が中止され、検証に失敗した以降のブロックは利用者に送信されないことになるため、結果として情報（または利用者が復号可能な暗号文）全てを不正に獲得してしまうことがないようにできる。

【０２８１】又、上記第４実施例によれば、大容量の情報を送信する場合に、第一に情報は情報提供者が生成した情報暗号化用秘密鍵によって初めに暗号化されて利用者に配送されるため、利用者の認証が行われる以前に情報本体を利用者が取り出すことはできない。第二に情報暗号化用秘密鍵についてのみ検査文として配送確認を行うことにより、通信量及び配送確認のための処理時間を大幅に短縮できる。第三に配送確認ステップが正常に終了すれば利用者は検査文を正しく受信したことが確認でき、情報取り出しステップにおいて情報暗号化用秘密鍵を獲得することが保証されるので、この時点で初めて情報を間違いなく取り出すことができる。したがって、これらの効果により情報配送方法が終了した場合には、情報提供者は正規の利用者に対して情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送し、かつ確実に利用者が受信したことが確認できるので、情報提供者は情報を利用者まで確実に配送したと判断できる。

【０２８２】又、一方向性関数を用いて情報暗号化用秘密鍵を生成することにより情報提供者にとって都合の良い情報暗号化用秘密鍵を不正に生成できないようにすることができる。また、同様に一方向性関数を用いることにより、乱数文と検査文と応答文とからなる通信履歴を偽造することは不可能になるので、情報提供者は正規の利用者に対して要求された情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送し、かつ確実に利用者が受信したことを後日証明できる証拠能力を持つことができる。

【０２８３】又、検査文について暗号通信を行うことは、情報暗号化用秘密鍵についても暗号通信を行なっていることと同等の効果が得られるため、第三者による情報暗号化用秘密鍵の盗聴を防止し、かつ第三者が情報暗号化用秘密鍵を解読するために有効な情報も得られないようにもなる。

【０２８４】又、検査文の復号処理を配送確認ステップと切り離して実行することができる。

【０２８５】又、例えば不正な利用者による利用などにより配送確認ステップの途中で情報提供者の検証に失敗した場合には、ただちにプロトコルの実行が中止され、検証に失敗した以降のブロックは利用者に送信されないことになる。したがって、情報提供者の検証を失敗させた利用者は暗号化された情報を復号するために必要な情報の一部しか獲得することができず、結果として情報本体もしくは情報暗号化用秘密鍵を生成することが不可能

となるので、不正な利用者が要求した情報を不正に獲得してしまうことがないようにできる。

【０２８６】又、上記第３、第４実施例によれば、偽造不可能な通信履歴を実際に情報を配送した証拠として記録管理することができ、かつ必要に応じて提示できるようになる。さらに、情報提供者が情報を配送した事実の証拠として記録管理しなければならない情報量が桜井（特開平５－１２３２１）の方式と比較して大幅に削減できる。

【０２８７】又、情報提供者と利用者の間で情報の提供の有無について調停を行う必要が生じた場合、情報提供者が通信履歴を裁判所等の中立な調停機関に提示し、調停機関が証拠能力を有する通信履歴についてその正当性を検査することにより、情報提供者と利用者のどちらの主張が正当であるのかを判定できる。すなわち、情報提供者が利用者に対して情報（または利用者が復号可能な暗号文）を送信し、かつ利用者が確実に受信したことを、後日調停者が確認できるので、利用者が情報（または利用者が復号可能な暗号文）を受信しているにも関わらず、利用者が情報を受信していないなどという不当な主張を防止できる。

【０２８８】又、上記第２～第４実施例によれば、情報提供者が要求された情報を利用者に確実に配送し、かつ利用者が確実に受信していることを情報提供者が確認できるシステムとなる。また、必要に応じて情報提供者が利用者を認証する利用者認証方法としてのゼロ知識証明プロトコルを単独に使用することもできる。

【０２８９】又、情報提供者と利用者の間で暗号通信ができるようにしたシステムとなる。

【０２９０】又、上記第４実施例によれば、情報提供者から提供された情報を蓄積し、利用者が必要に応じて情報を利用できるようにしたシステムとなる。

【０２９１】又、情報暗号化用秘密鍵の生成機能を有し、情報暗号化用秘密鍵を用いた情報配送ができようにしたシステムとなる。

【０２９２】又、上記第３、第４実施例によれば、証拠能力を有する通信履歴を必要に応じて提示できるようにしたシステムとなる。

【０２９３】又、不正な利用者であることを検出した際には直ちにプロトコルの実行を中止して、不正な利用者が要求した情報を不正に獲得してしまうことがないようにしたシステムとなる。

【０２９４】又、裁判所等の中立な調停機関により、証拠能力を有する通信履歴についてその正当性を検査し、情報提供者と利用者のどちらの主張が正当であるのかを判定することができるようにしたシステムとなる。

【０２９５】一方、上記第５～第８実施例によれば、ゼロ知識証明プロトコルを利用した情報配送方法では、第一に情報配送ステップにおいて、利用者が要求した情報は情報提供者によって暗号化されて利用者に配送されるため、この時点では要求した情報そのものを利用者が取り出すことはできない。第二に配送確認ステップで行われるプロトコル動作自体は利用者認証としてのゼロ知識証明プロトコルと同等であるため、ゼロ知識証明プロトコルと同じように不正な利用者が情報提供者の検証をクリアすることはほぼ不可能である。第三に配送確認ステップが正常に終了した場合には、ゼロ知識証明プロトコルが正常に終了したことと同値であるから、情報提供者は利用者が検査文を正しく受信し、適正な処理をしていると判断できる。第四に情報取り出しステップにおいて、利用者は検査文を正しく受信できれば、秘密鍵配送文及び情報暗号化用秘密鍵を作成することができるので、この時点で前記情報暗号化用秘密鍵により暗号化された情報を復号し、要求した情報を取り出すことができる。したがって、これらの効果により、情報配送方法の全てのステップが終了した場合には、情報提供者は正規の利用者に対して要求された情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送し、かつ確実に利用者が受信したことが確認できるので、情報提供者は利用者が要求した情報を利用者まで確実に配送したと判断できる。

【０２９６】又、上記第５、第６実施例によれば、検査文について暗号通信をすることは、情報暗号化用秘密鍵についても暗号通信をしていることと同等の効果が得られることになり、第三者が通信路を盗聴したとしてもこれらの秘密鍵が知られることはない。さらに、情報暗号化用秘密鍵を解読するために有効な情報も得られないようにすることもできる。

【０２９７】又、上記第７、第８実施例によれば、情報提供者にとって都合のよい情報暗号化用秘密鍵を不正に作成できないようにすることができる。

【０２９８】又、通信履歴を偽造することは不可能であるので、情報提供者は正規の利用者に対して要求された情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送し、かつ確実に利用者が受信したことを後日証明できる証拠能力を持つことができる。

【０２９９】又、証拠能力を有する通信履歴を必要に応じて提示できるようになる。また、情報提供者が情報を配送した事実の証拠として記録管理しなければならない情報量が桜井（特開平５－１２３２１）の方式と比較して大幅に削減できる。

【０３００】又、情報提供者と利用者の間で情報の提供の有無について調停をする必要が生じた場合、裁判所等の中立な調停機関が証拠能力を有する通信履歴についてその正当性を検査することにより、情報提供者と利用者のどちらの主張が正当であるのかを判定できる。

【０３０１】又、上記第８実施例によれば、情報配送要求文を暗号送信することにより、第三者による情報配送要求文の盗聴を防止し、どんな情報を要求したかなどの

利用者のプライバシーが保護できる。

【０３０２】又、鍵暗号化用秘密鍵及び情報暗号化用秘密鍵については、情報提供者と利用者のみの秘密の情報によりスクランブルされるので、第三者が通信路を盗聴したとしてもこれらの秘密鍵が知られることはなく、また秘密鍵を解読するために有効な情報も得られない。したがって、利用者が要求した情報を第三者が不正に獲得することはできない。

【０３０３】又、例えば不正な利用者による利用などにより配送確認ステップの途中で情報提供者の検証に失敗した場合には、ただちにプロトコルの実行が中止され、検証に失敗した以降のブロックは利用者に送信されないことになる。したがって、情報提供者の検証を失敗させた利用者は暗号化された情報を復号するために必要な情報の一部しか獲得することができず、結果として鍵暗号化用秘密鍵もしくは情報暗号化用秘密鍵を生成することが不可能となるので、不正な利用者が要求した情報を不正に獲得してしまうことがないようにできる。

【０３０４】又、上記第５～第８実施例によれば、情報提供者が要求された情報を利用者に確実に配送し、かつ利用者が確実に受信していることを情報提供者が確認できるシステムとなる。また、必要に応じて情報提供者が利用者を認証する利用者認証方法としてのゼロ知識証明プロトコルを単独に使用することもできる。

【０３０５】又、情報暗号化秘密鍵を生成するときに乱数文を利用できるようにしたシステムとなる。

【０３０６】又、上記第５、第８実施例によれば、情報提供者が秘密に保持すべき情報を蓄積することができる情報提供者秘密情報蓄積手段を有したシステムとなる。

【０３０７】又、上記第５、第６、第８実施例によれば、情報提供者と利用者の間で公開鍵暗号方法による暗号通信ができるようにしたシステムとなる。

【０３０８】又、上記第７、第８実施例によれば、情報配送要求文を簡単に作成するための入力手段を利用者端末に備えたシステムとなる。

【０３０９】又、鍵暗号化用秘密鍵と秘密鍵配送文との生成機能を有し、情報暗号化用秘密鍵と鍵暗号用秘密鍵とを利用した情報配送ができるようにしたシステムとなる。

【０３１０】又、証拠能力を有する通信履歴を必要に応じて提示できるようにしたシステムとなる。

【０３１１】又、裁判所等の中立な調停機関により、証拠能力を有する通信履歴についてその正当性を検査し、情報提供者と利用者のどちらの主張が正当であるのかを判定することができるようにしたシステムとなる。

【０３１２】又、上記第８実施例によれば、不正な利用者があることを検出した際には直ちにプロトコルの実行を中止して、不正な利用者が要求した情報を不正に獲得してしまうことがないようにしたシステムとなる。

【０３１３】一方、上記第９実施例によれば、ゼロ知識証明プロトコルを利用した情報配送方法では、第一に情報配送ステップにおいて、利用者が要求した情報は情報提供者によって暗号化されて利用者に配送されるため、この時点では要求した情報そのものを利用者が取り出すことはできない。第二に配送確認ステップで行われるプロトコル動作自体は利用者認証としてのゼロ知識証明プロトコルと同等であるため、ゼロ知識証明プロトコルと同じように不正な利用者が情報提供者の検証をクリアすることはほぼ不可能である。第三に配送確認ステップが正常に終了した場合には、ゼロ知識証明プロトコルが正常に終了したことと同値であるから、情報提供者は利用者が検査文を正しく受信し、適正な処理をしていると判断できる。第四に情報取り出しステップにおいて、利用者は検査文を正しく受信できれば情報暗号化用秘密鍵を作成することができるので、この時点で前記情報暗号化用秘密鍵により暗号化された情報を復号し、要求した情報を取り出すことができる。したがって、これらの効果により、情報配送方法の全てのステップが終了した場合には、情報提供者は正規の利用者に対して要求された情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送し、かつ確実に利用者が受信したことが確認できるので、情報提供者は利用者が要求した情報を利用者まで確実に配送したと判断できる。

【０３１４】又、情報提供者が自分に都合のよい情報暗号化用秘密鍵に不正に改竄できないようにすることができる。さらに、暗号化された情報暗号化用秘密鍵は情報提供者以外は復号することができないので、署名を行う時点では利用者に情報暗号化用秘密鍵を知られることはない。

【０３１５】又、通信履歴を偽造することは不可能であるので、情報提供者は正規の利用者に対して要求された情報を暗号化した状態で提供した後、利用者が暗号化された情報を復号するために必要な情報を利用者に配送し、かつ確実に利用者が受信したことを後日証明できる証拠能力を持つことができる。

【０３１６】又、証拠能力を有する通信履歴を必要に応じて提示できるようになる。また、情報提供者が情報を配送した事実の証拠として記録管理しなければならない情報量が桜井（特開平５－１２３２１）の方式と比較して大幅に削減できる。

【０３１７】又、情報提供者と利用者の間で情報の提供の有無について調停をする必要が生じた場合、裁判所等の中立な調停機関が証拠能力を有する通信履歴についてその正当性を検査することにより、情報提供者と利用者のどちらの主張が正当であるのかを判定できる。

【０３１８】又、例えば不正な利用者による利用などにより配送確認ステップの途中で情報提供者の検証に失敗した場合には、ただちにプロトコルの実行が中止され、検証に失敗した以降のブロックは利用者に送信されない

ことになる。したがって、情報提供者の検証を失敗させた利用者は暗号化された情報を復号するために必要な情報の一部しか獲得することができず、結果として情報暗号化用秘密鍵を生成することが不可能となるので、不正な利用者が要求した情報を不正に獲得してしまうことがないようにできる。

【０３１９】又、上記第９実施例によれば、情報提供者が要求された情報を利用者に確実に配送し、かつ利用者が確実に受信していることを情報提供者が確認できるシステムとなる。また、必要に応じて情報提供者が利用者を認証する利用者認証方法としてのゼロ知識証明プロトコルを単独に使用することもできる。

【０３２０】又、情報暗号化秘密鍵を生成するときに乱数文を利用できるようにしたシステムとなる。

【０３２１】又、情報提供者が秘密に保持すべき情報を蓄積することができる情報提供者秘密情報蓄積手段を有したシステムとなる。

【０３２２】又、情報提供者と利用者の間で公開鍵暗号方法による暗号通信ができるようにしたシステムとなる。

【０３２３】又、鍵暗号化用秘密鍵と生成機能を有し、情報暗号化用秘密鍵と鍵暗号用秘密鍵とを利用した情報配送ができるようにしたシステムとなる。

【０３２４】又、証拠能力を有する通信履歴を必要に応じて提示できるようにしたシステムとなる。

【０３２５】又、裁判所等の中立な調停機関により、証拠能力を有する通信履歴についてその正当性を検査し、情報提供者と利用者のどちらの主張が正当であるのかを判定することができるようにしたシステムとなる。

【０３２６】又、不正な利用者があることを検出した際には直ちにプロトコルの実行を中止して、不正な利用者が要求した情報を不正に獲得してしまうことがないようにしたシステムとなる。

【図面の簡単な説明】

【図１】従来のFiat Shamir 法による利用者認証方式と、従来の認証子法によるメッセージ認証方式と、従来のＲＳＡ署名法によるディジタル署名方式を示す概念図である。

【図２】本発明の第１実施例における情報配送システムの構成例を示すブロック図である。

【図３】図２に示す情報配送システムの動作手順を示すフローチャートである。

【図４】図２に示す情報配送システムで用いる配送情報の例を示す模式図である。

【図５】本発明の第２実施例における情報配送システムの構成例を示すブロック図である。

【図６】図５に示す情報配送システムの動作手順を示すフローチャートである。

【図７】本発明の第３実施例における情報配送システムの構成例を示すブロック図である。

【図８】図７に示す情報配送システムの配送確認に関する動作手順を示すフローチャートである。

【図９】図７に示す情報配送システムの調停に関する動作手順を示すフローチャートである。

【図１０】本発明の第４実施例における情報配送システムの構成例を示すブロック図である。

【図１１】図１０に示す情報配送システムの配送確認と情報取り出しに関する動作手順を示すフローチャートである。

【図１２】図１０に示す情報配送システムの調停に関する動作手順を示すフローチャートである。

【図１３】本発明の第５実施例における情報配送システムの構成例を示すブロック図である。

【図１４】図１３に示す情報配送システムの動作手順を示すフローチャートである。

【図１５】本発明の第６実施例における情報配送システムの構成例を示すブロック図である。

【図１６】図１５に示す情報配送システムの動作手順を示すフローチャートである。

【図１７】本発明の第７実施例における情報配送システムの構成例を示すブロック図である。

【図１８】図１７に示す情報配送システムの情報配送、配送確認、情報取り出しに関する動作手順を示すフローチャートである。

【図１９】図１７に示す情報配送システムの調停に関する動作手順を示すフローチャートである。

【図２０】図１７に示す情報配送システムで用いる情報配送要求文の構成形態を示す模式図である。

【図２１】図１７に示す情報配送システムで用いる通信履歴の構成形態を示す模式図である。

【図２２】本発明の第８実施例における情報配送システムの構成例を示すブロック図である。

【図２３】図２２に示す情報配送システムの情報配送、配送確認、情報取り出しに関する動作手順の前半を示すフローチャートである。

【図２４】図２２に示す情報配送システムの情報配送、配送確認、情報取り出しに関する動作手順の後半を示すフローチャートである。

【図２５】図２２に示す情報配送システムの調停に関する動作手順を示すフローチャートである。

【図２６】本発明の第９実施例における情報配送システムの構成例を示すブロック図である。

【図２７】図２６に示す情報配送システムの情報配送、配送確認、情報取り出しに関する動作手順の前半を示すフローチャートである。

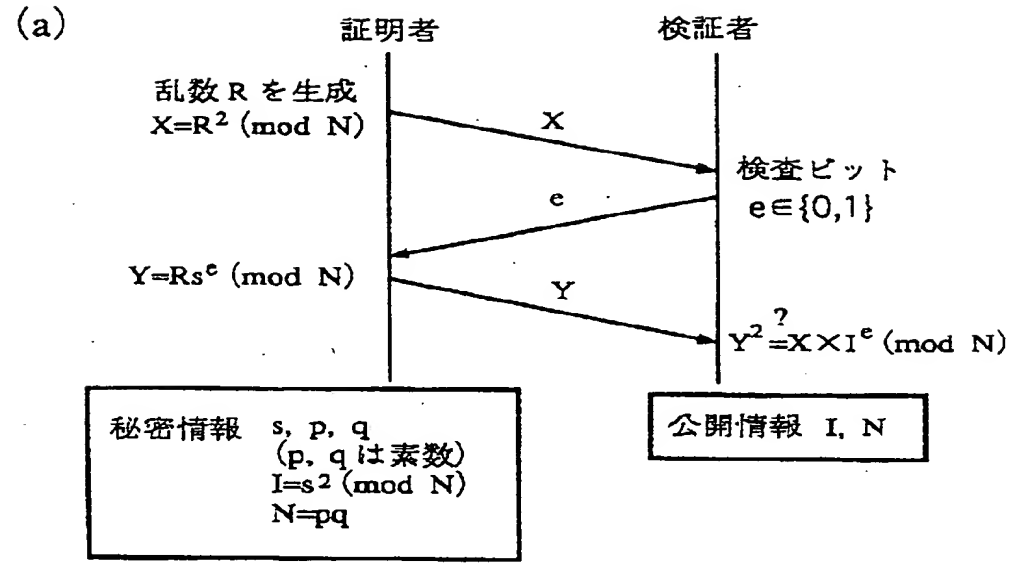
【図２８】図２６に示す情報配送システムの情報配送、配送確認、情報取り出しに関する動作手順の後半を示すフローチャートである。

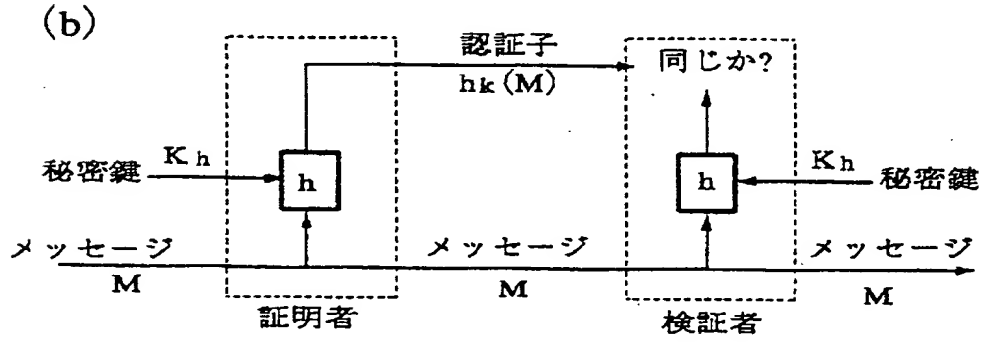
【図２９】図２６に示す情報配送システムの調停に関する動作手順を示すフローチャートである。

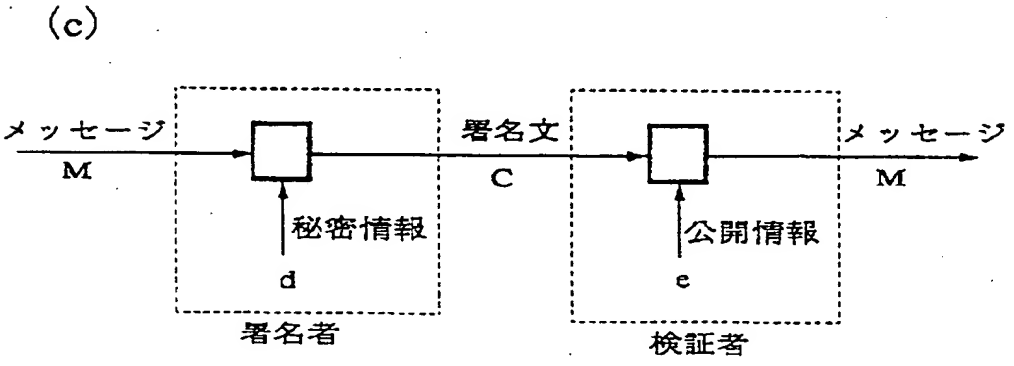
【符号の説明】

１　カード
１１　秘密情報蓄積手段
１２　乱数発生手段
１３　演算手段
１４　蓄積手段
２　利用者端末
２１　カード挿入手段
２２　蓄積手段
２３　利用手段
２４　通信制御手段
３　情報提供者端末
３１　情報蓄積手段
３２　情報分割手段
３３　検証手段
３４　履歴管理手段
３５　通信制御手段
５０　配送情報
１０　利用者端末
２０　情報提供者端末
３０　通信回線
４０　調停者端末
１００　通信制御手段
１０１　利用者秘密情報蓄積手段
１０２　一時メモリ
１０３　乱数発生手段
１０４　演算手段
１０５　共通鍵暗号手段
１０６　情報出力／利用手段
１０７　公開鍵暗号手段
１０８　情報再構成手段
１０９　情報蓄積手段
１１０　入力手段
４１　演算手段
４２　一時メモリ
４３　検証手段
４４　情報分割手段
４５　公開鍵暗号手段
２００　通信制御手段
２０１　情報提供者秘密情報蓄積手段
２０２　情報データベース
２０３　一時メモリ
２０４　演算手段
２０５　共通鍵暗号手段
２０６　検証手段
２０７　情報分割手段
２０８　通信履歴ファイル
２０９　乱数発生手段
２１０　公開鍵暗号手段
４０１　演算手段
４０２　一時メモリ
４０３　検証手段
４０４　情報分割手段
４０５　公開鍵暗号手段

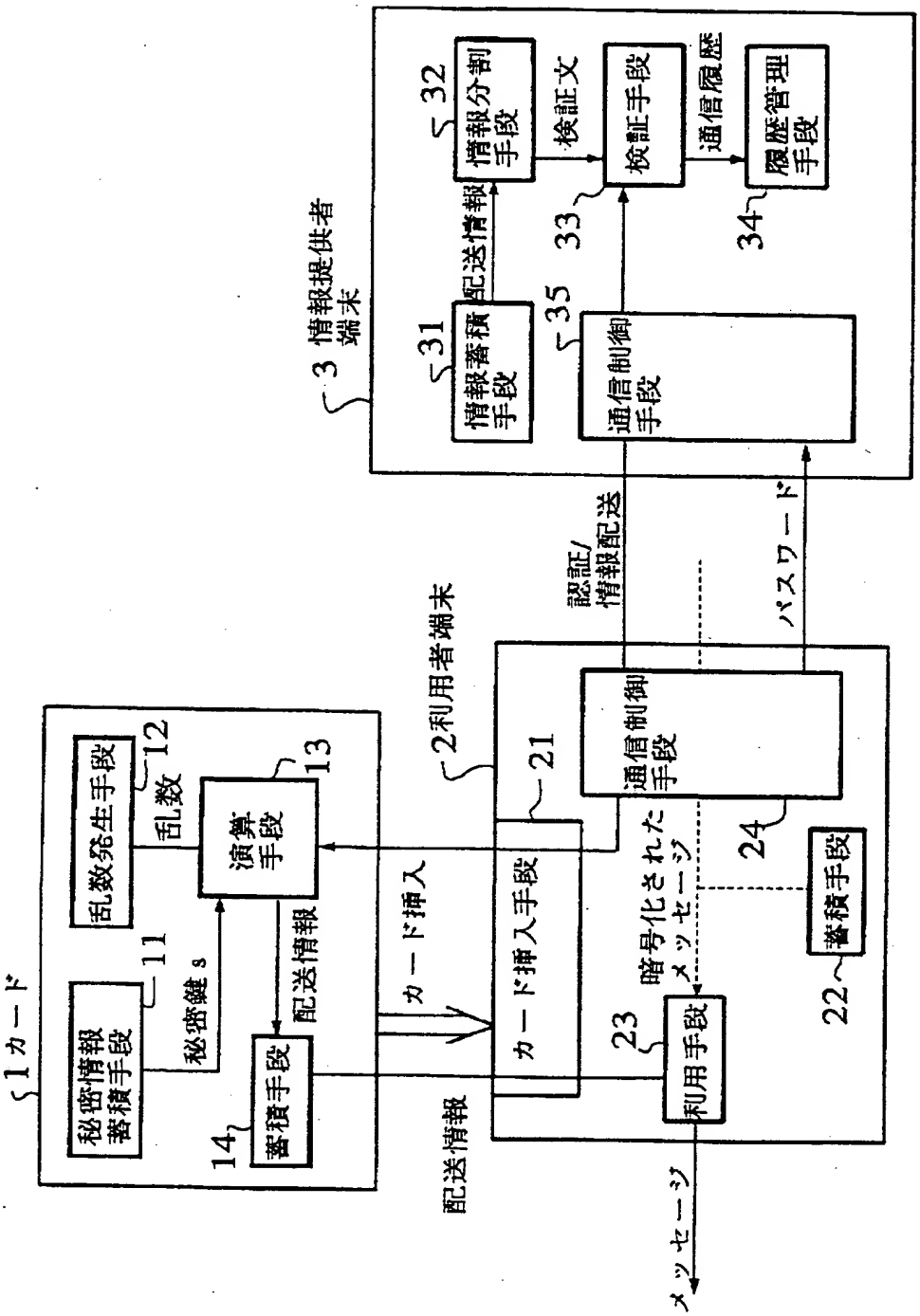
【図１】


(a)
証明者
検証者
乱数Rを生成
X=R² (mod N)
X
検査ビット
e∈{0,1}
e
Y=Rs^e (mod N)
Y
Y² =? X×I^e (mod N)
秘密情報　s, p, q
(p, qは素数)
I=s² (mod N)
N=pq
公開情報　I, N

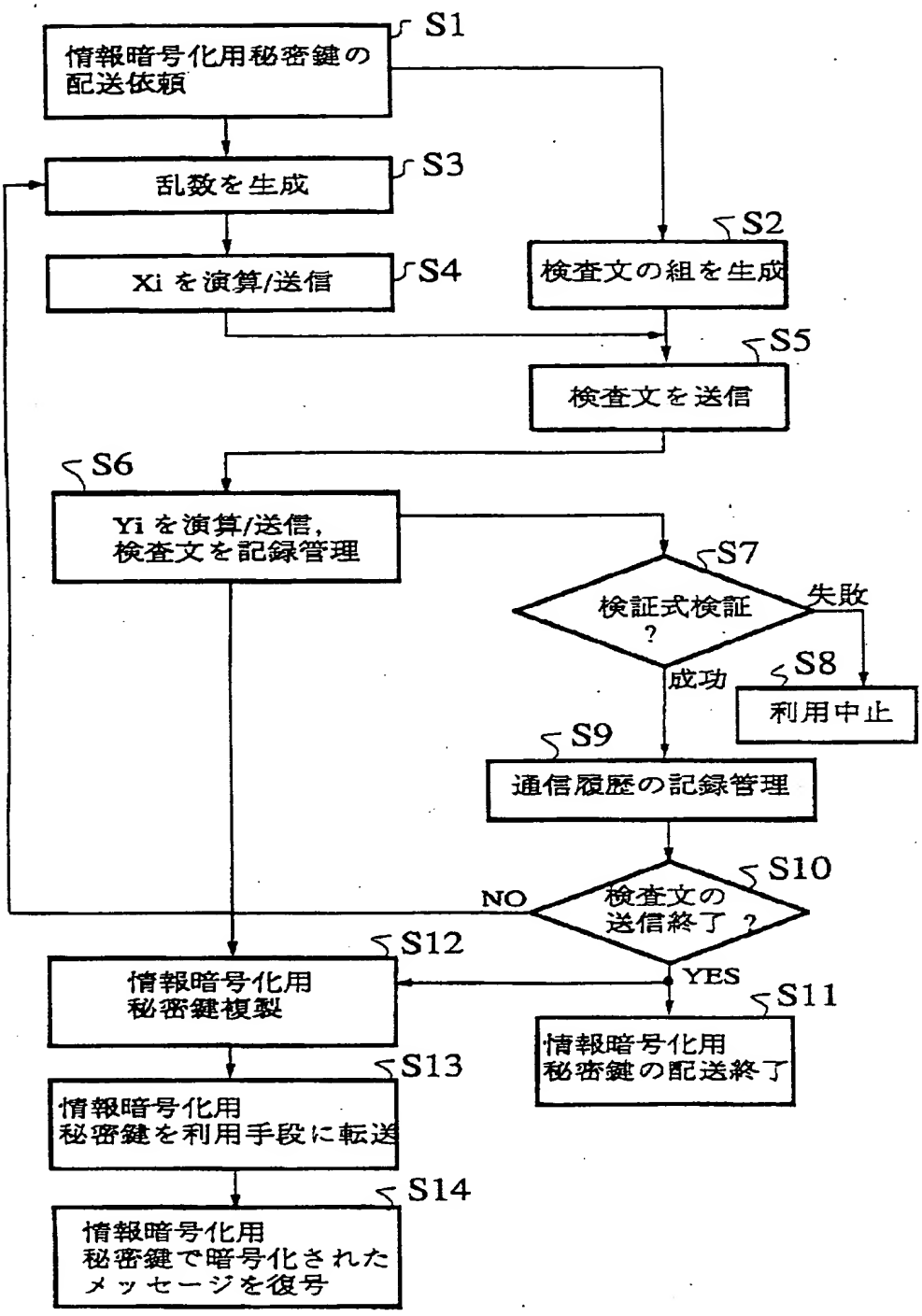

(b)
認証子
hk(M)
同じか?
秘密鍵
Kh
h
Kh
秘密鍵
メッセージ
M
メッセージ
M
メッセージ
M
証明者
検証者


(c)
メッセージ
M
署名文
C
メッセージ
M
秘密情報
d
公開情報
e
署名者
検証者

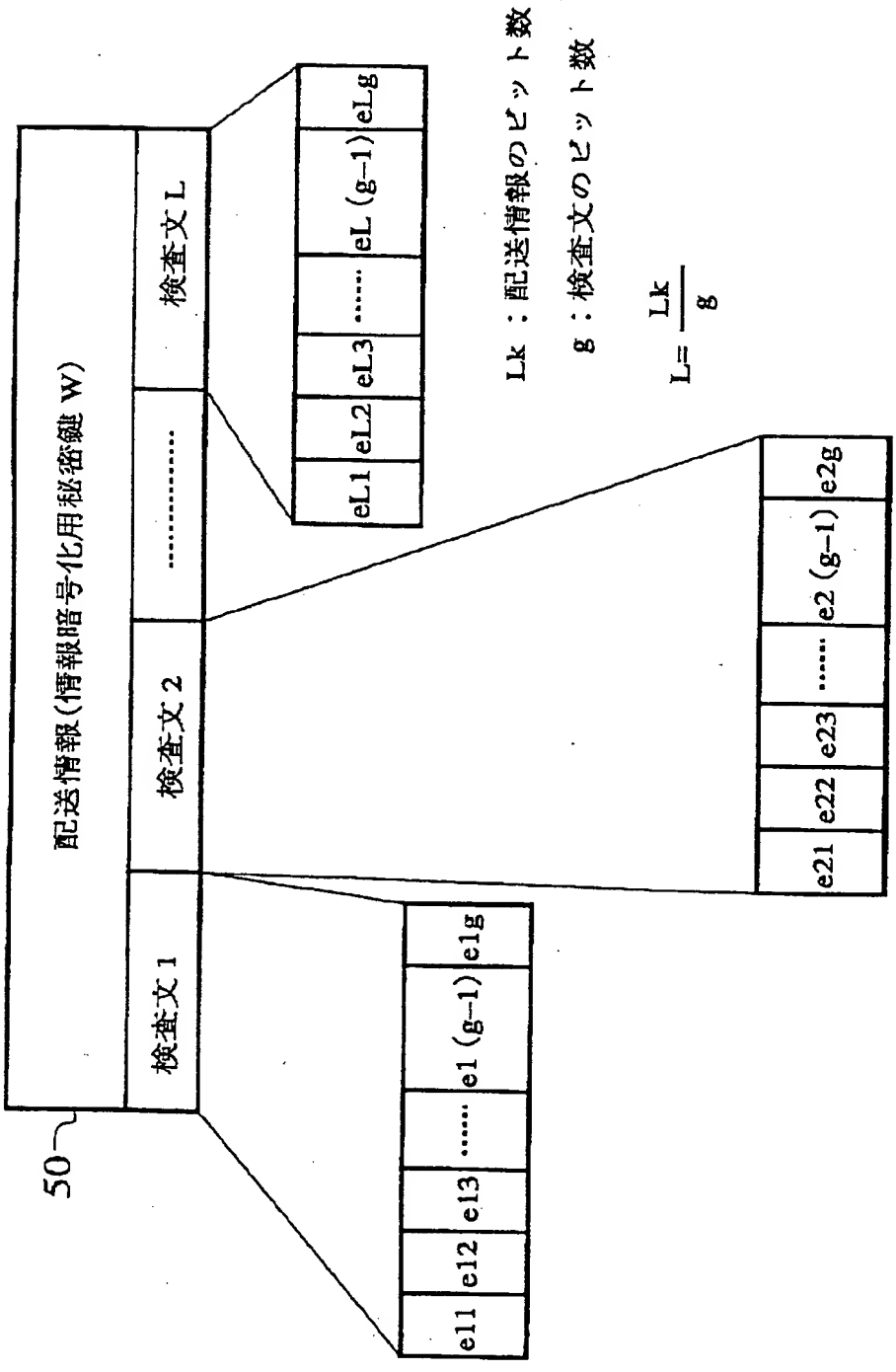
【図2】


1カード
秘密情報蓄積手段
11
乱数発生手段
12
乱数
秘密鍵s
演算手段
13
配送情報
14
蓄積手段
カード挿入
配送情報
2利用者端末
カード挿入手段
21
通信制御手段
暗号化されたメッセージ
23
利用手段
24
蓄積手段
22
認証/情報配送
パスワード
メッセージ
3 情報提供者端末
31
情報蓄積手段
配送情報
32
情報分割手段
検証文
検証手段
33
通信履歴
履歴管理手段
34
35
通信制御手段

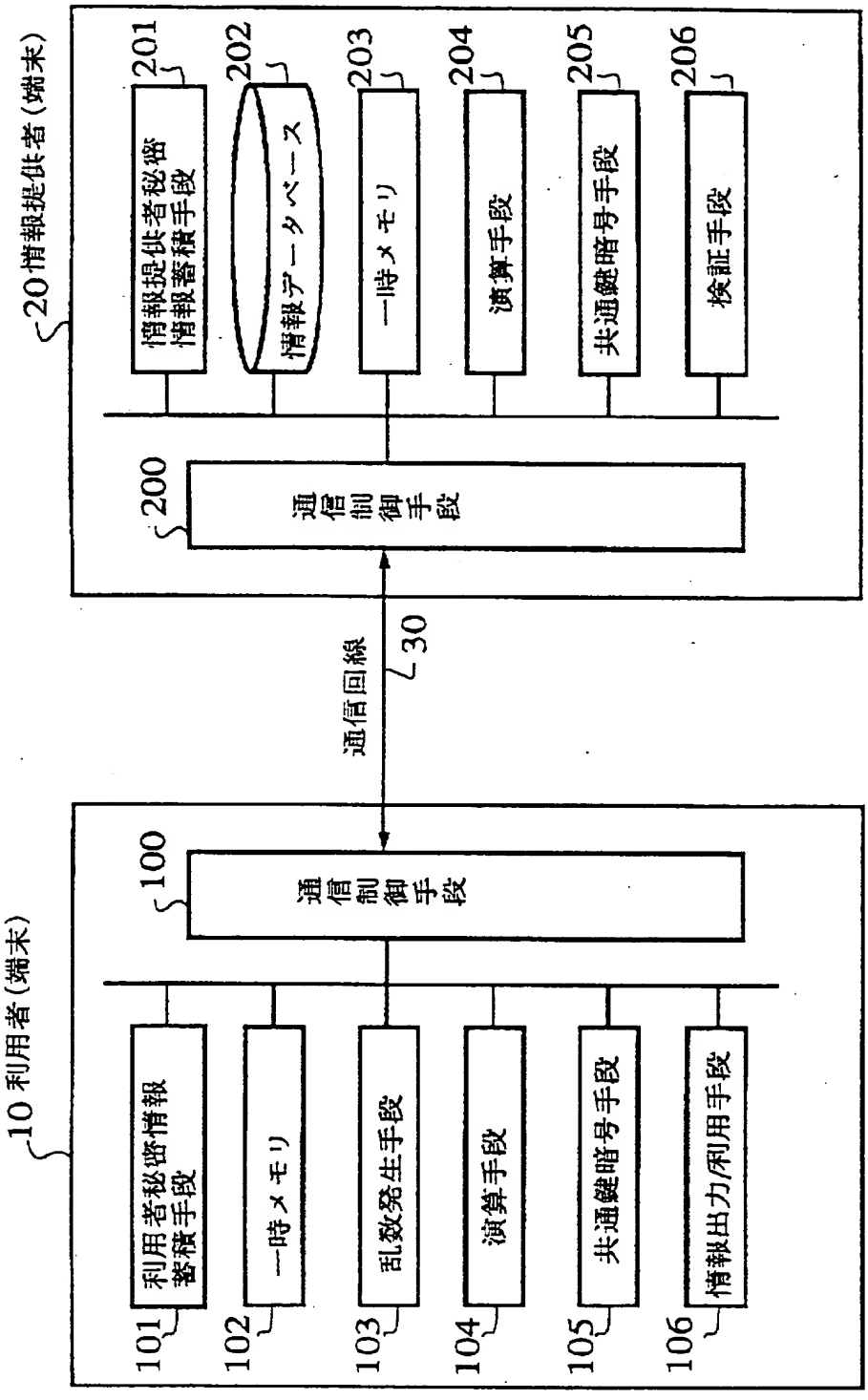
【図３】


S1
情報暗号化用秘密鍵の配送依頼
S3
乱数を生成
S2
検査文の組を生成
S4
Xi を演算/送信
S5
検査文を送信
S6
Yi を演算/送信，検査文を記録管理
S7
検証式検証 ?
失敗
成功
S8
利用中止
S9
通信履歴の記録管理
S10
検査文の送信終了 ?
NO
YES
S12
情報暗号化用秘密鍵複製
S11
情報暗号化用秘密鍵の配送終了
S13
情報暗号化用秘密鍵を利用手段に転送
S14
情報暗号化用秘密鍵で暗号化されたメッセージを復号

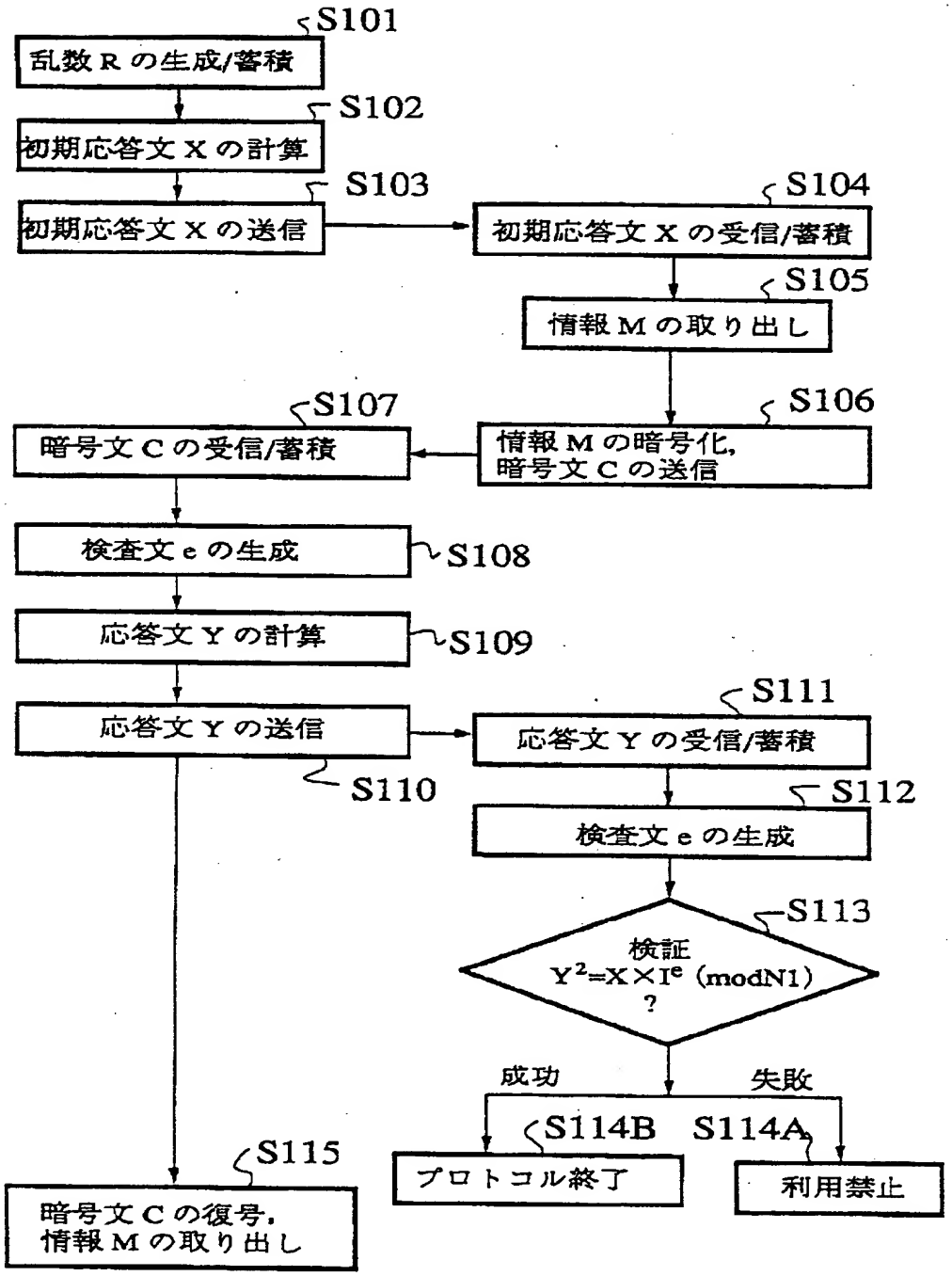
【図４】


配送情報(情報暗号化用秘密鍵 W)
検査文 1
検査文 2
.....
検査文 L
50
e11 e12 e13 ..... e1 (g−1) e1g
e21 e22 e23 ..... e2 (g−1) e2g
eL1 eL2 eL3 ..... eL (g−1) eLg
Lk：配送情報のビット数
g：検査文のビット数
L= Lk / g

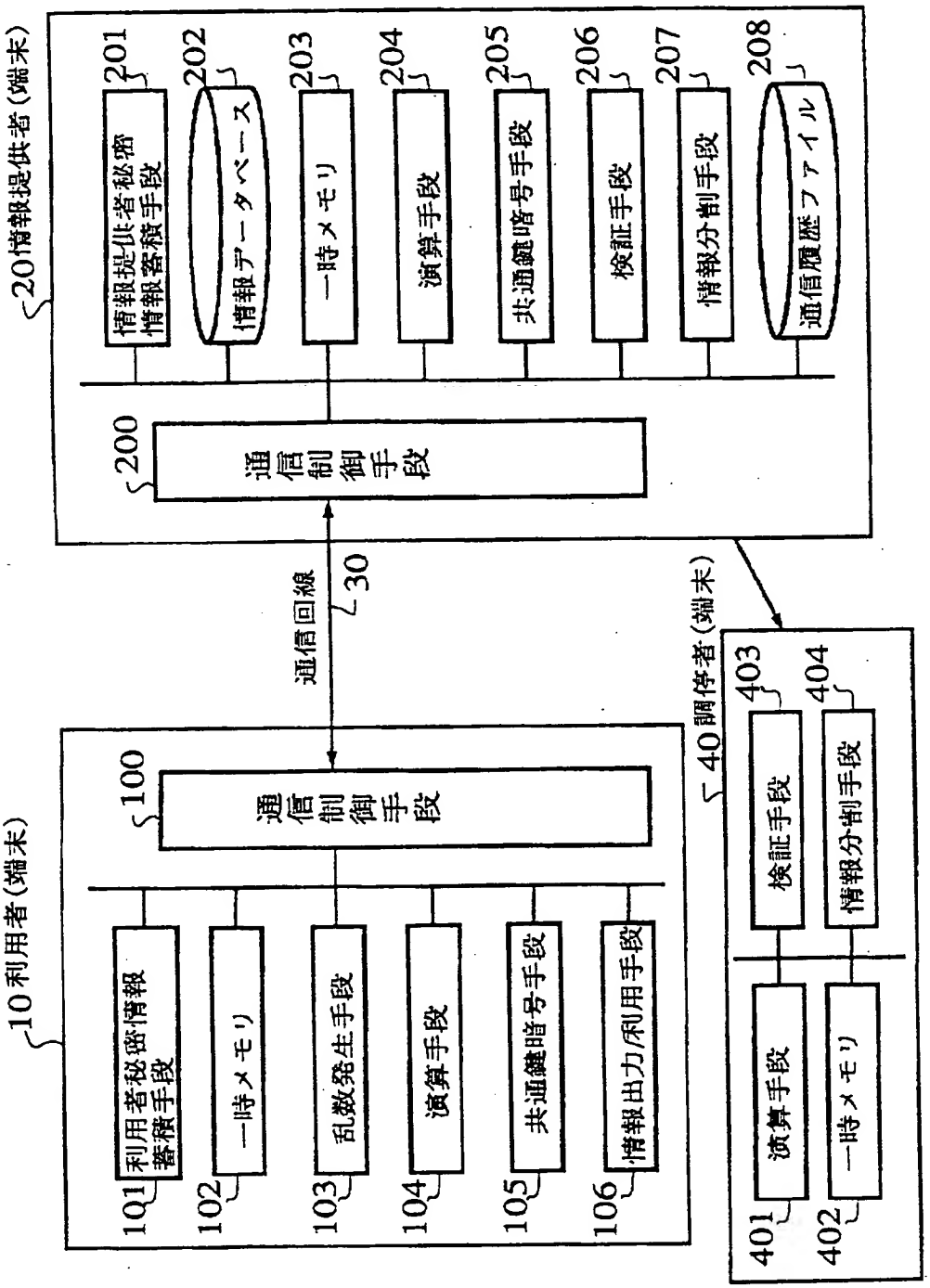
【図5】


10 利用者(端末)
20 情報提供者(端末)
30
通信回線
100
通信制御手段
101
利用者秘密情報蓄積手段
102
一時メモリ
103
乱数発生手段
104
演算手段
105
共通鍵暗号手段
106
情報出力/利用手段
200
通信制御手段
201
情報提供者秘密情報蓄積手段
202
情報データベース
203
一時メモリ
204
演算手段
205
共通鍵暗号手段
206
検証手段

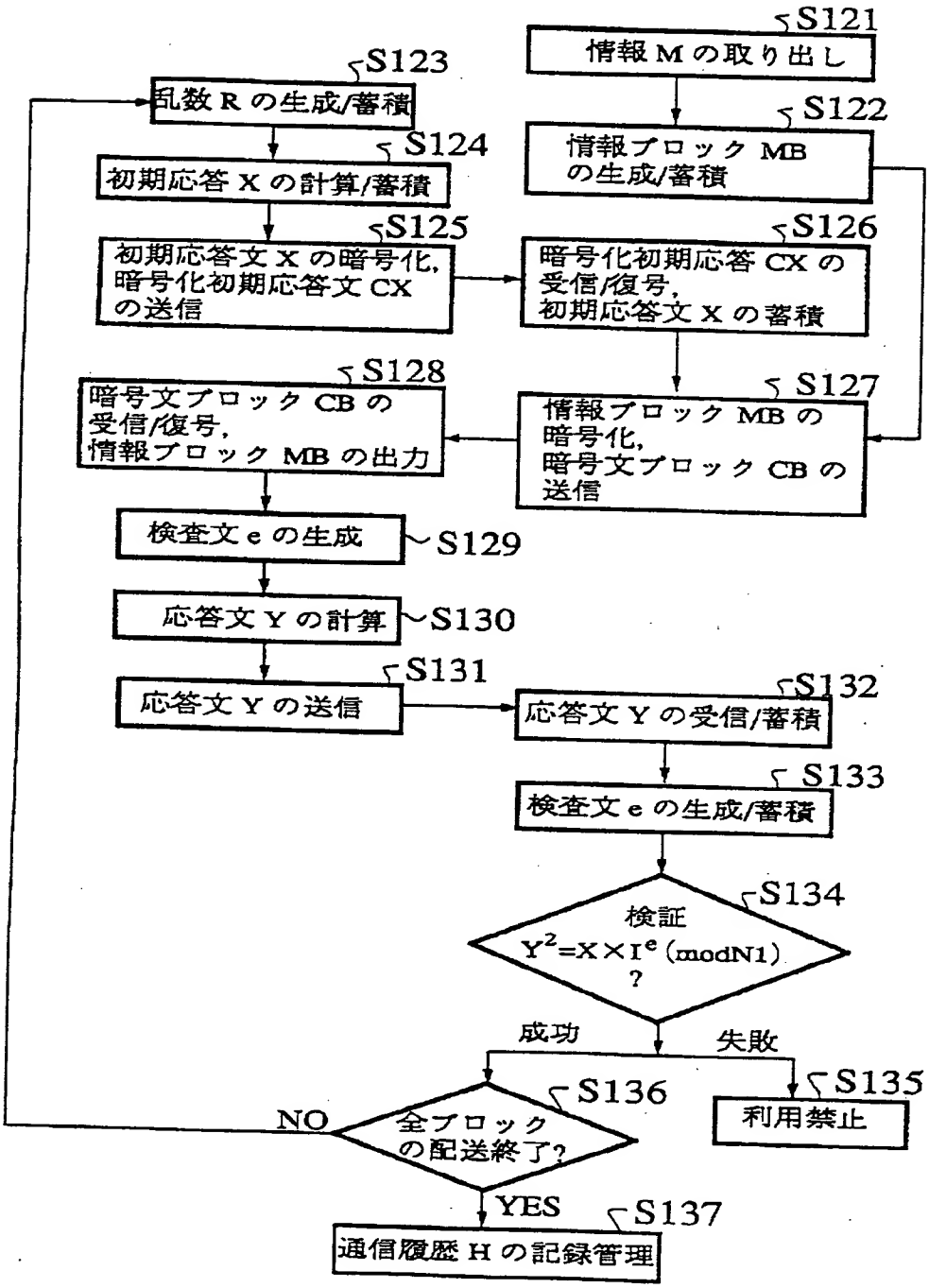
【図6】


S101
乱数Rの生成/蓄積
S102
初期応答文Xの計算
S103
初期応答文Xの送信
S104
初期応答文Xの受信/蓄積
S105
情報Mの取り出し
S106
情報Mの暗号化,
暗号文Cの送信
S107
暗号文Cの受信/蓄積
検査文eの生成
S108
応答文Yの計算
S109
応答文Yの送信
S110
S111
応答文Yの受信/蓄積
S112
検査文eの生成
S113
検証
$Y^2=X\times I^e$ (modN1)
?
成功
失敗
S114B
S114A
プロトコル終了
利用禁止
S115
暗号文Cの復号,
情報Mの取り出し

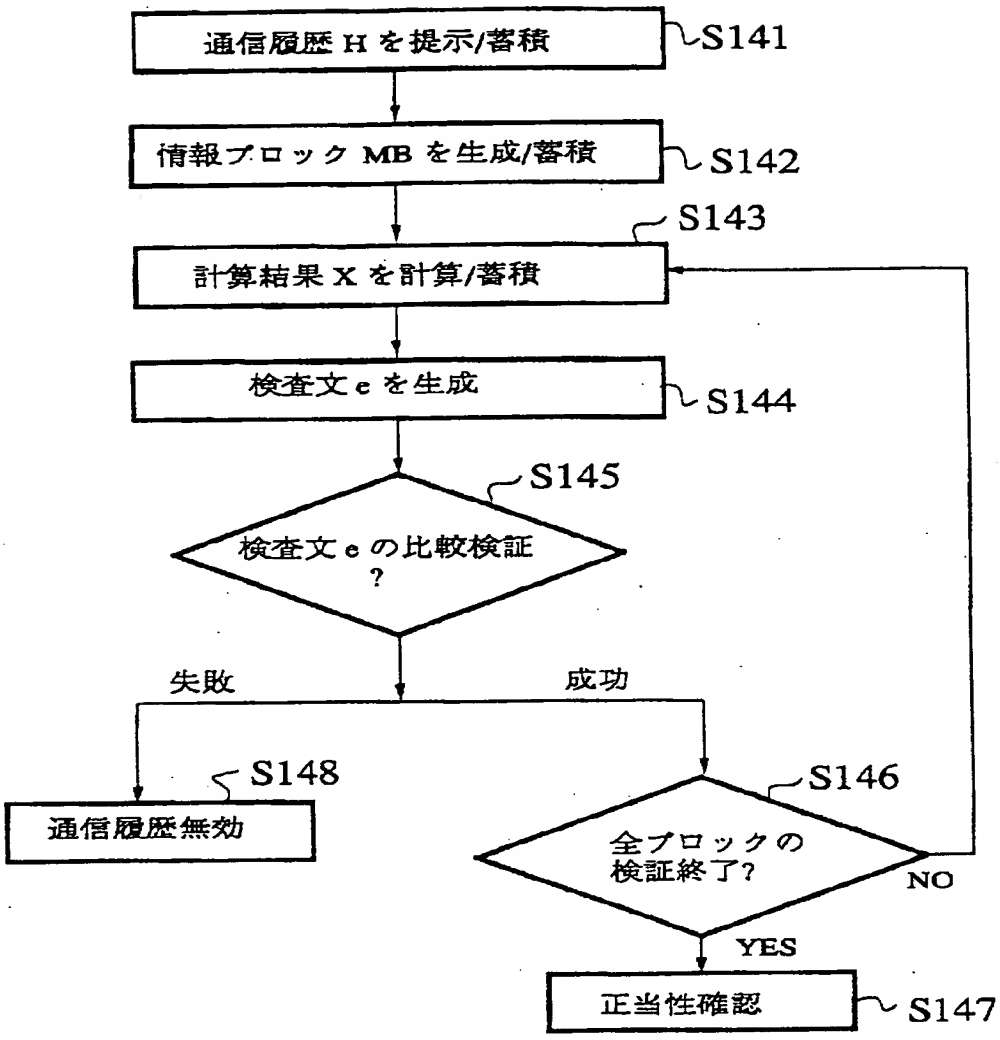
【図7】


20情報提供者(端末)
201
情報提供者秘密情報蓄積手段
202
情報データベース
203
一時メモリ
204
演算手段
205
共通鍵暗号手段
206
検証手段
207
情報分割手段
208
通信履歴ファイル
200
通信制御手段
30
通信回線
10利用者(端末)
100
通信制御手段
101
利用者秘密情報蓄積手段
102
一時メモリ
103
乱数発生手段
104
演算手段
105
共通鍵暗号手段
106
情報出力/利用手段
40調停者(端末)
403
検証手段
404
情報分割手段
401
演算手段
402
一時メモリ

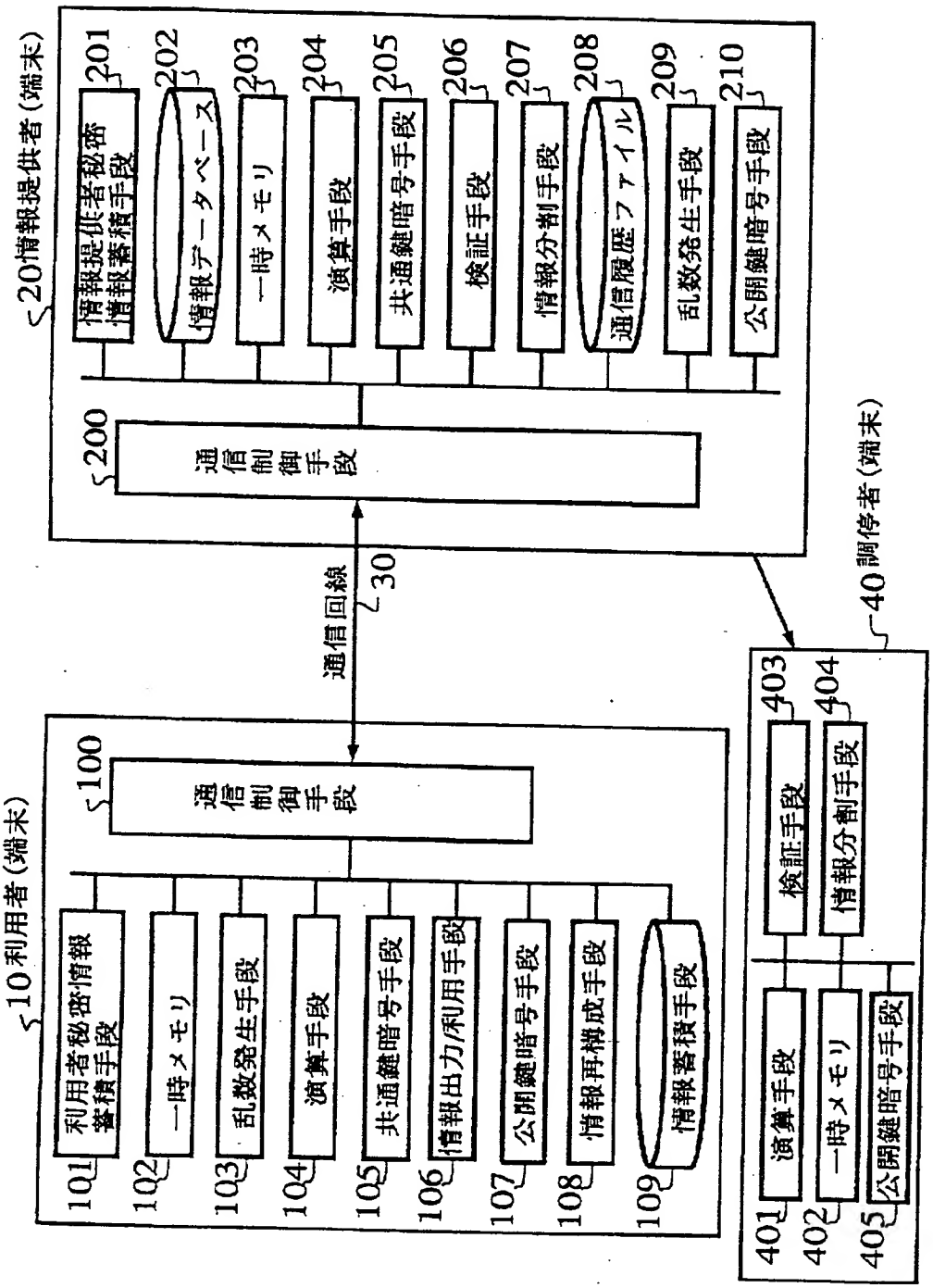
【図８】


S121
情報Mの取り出し
S122
情報ブロックMBの生成/蓄積
S123
乱数Rの生成/蓄積
S124
初期応答Xの計算/蓄積
S125
初期応答文Xの暗号化,暗号化初期応答文CXの送信
S126
暗号化初期応答CXの受信/復号,初期応答文Xの蓄積
S127
情報ブロックMBの暗号化,暗号文ブロックCBの送信
S128
暗号文ブロックCBの受信/復号,情報ブロックMBの出力
S129
検査文eの生成
S130
応答文Yの計算
S131
応答文Yの送信
S132
応答文Yの受信/蓄積
S133
検査文eの生成/蓄積
S134
検証
$Y^2=X\times I^e \pmod{N1}$
?
成功
失敗
S135
利用禁止
S136
全ブロックの配送終了?
NO
YES
S137
通信履歴Hの記録管理

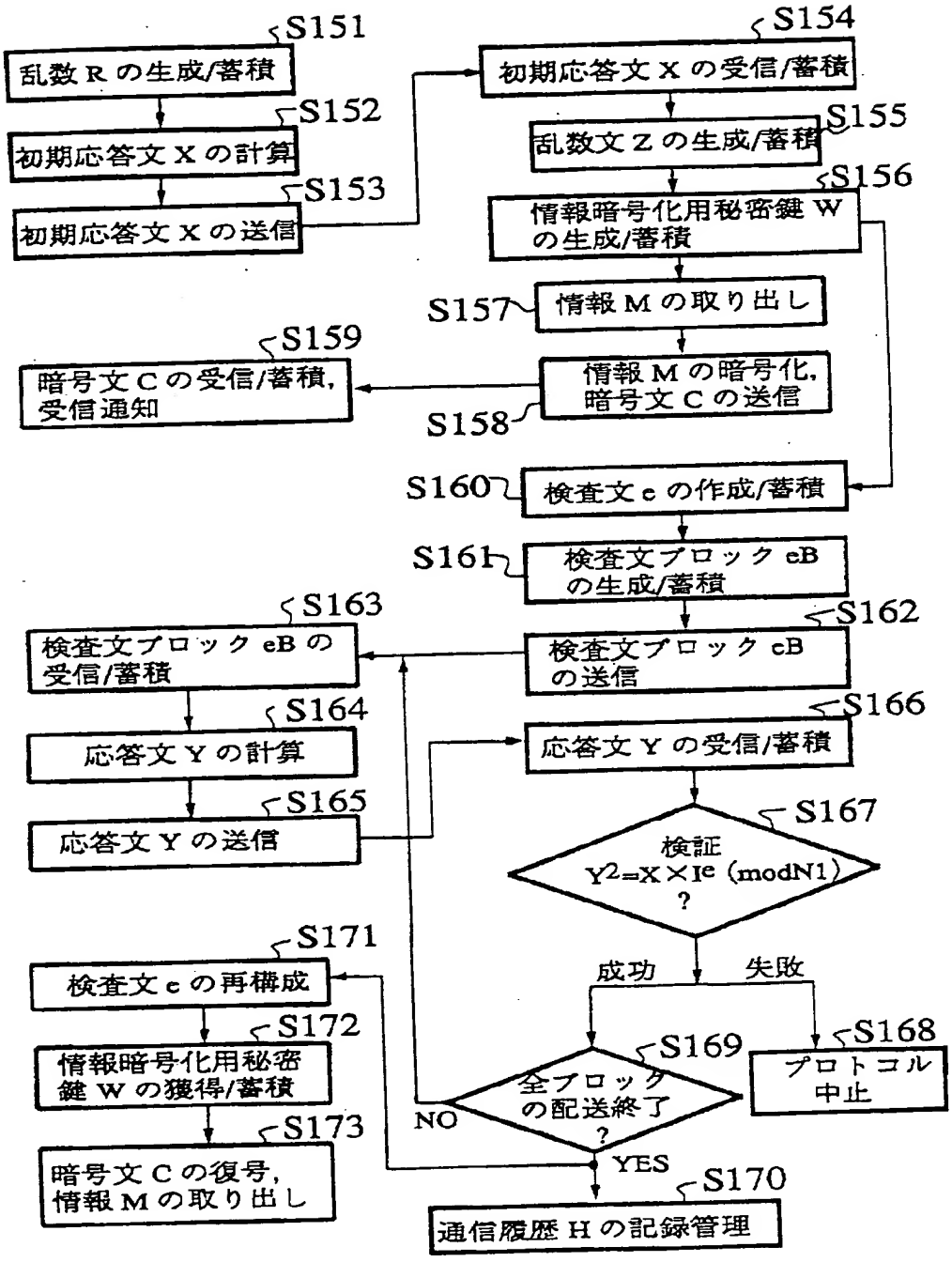
【図9】


通信履歴Hを提示/蓄積
S141
情報ブロックMBを生成/蓄積
S142
S143
計算結果Xを計算/蓄積
検査文eを生成
S144
S145
検査文eの比較検証?
失敗
成功
S148
通信履歴無効
S146
全ブロックの検証終了?
NO
YES
正当性確認
S147

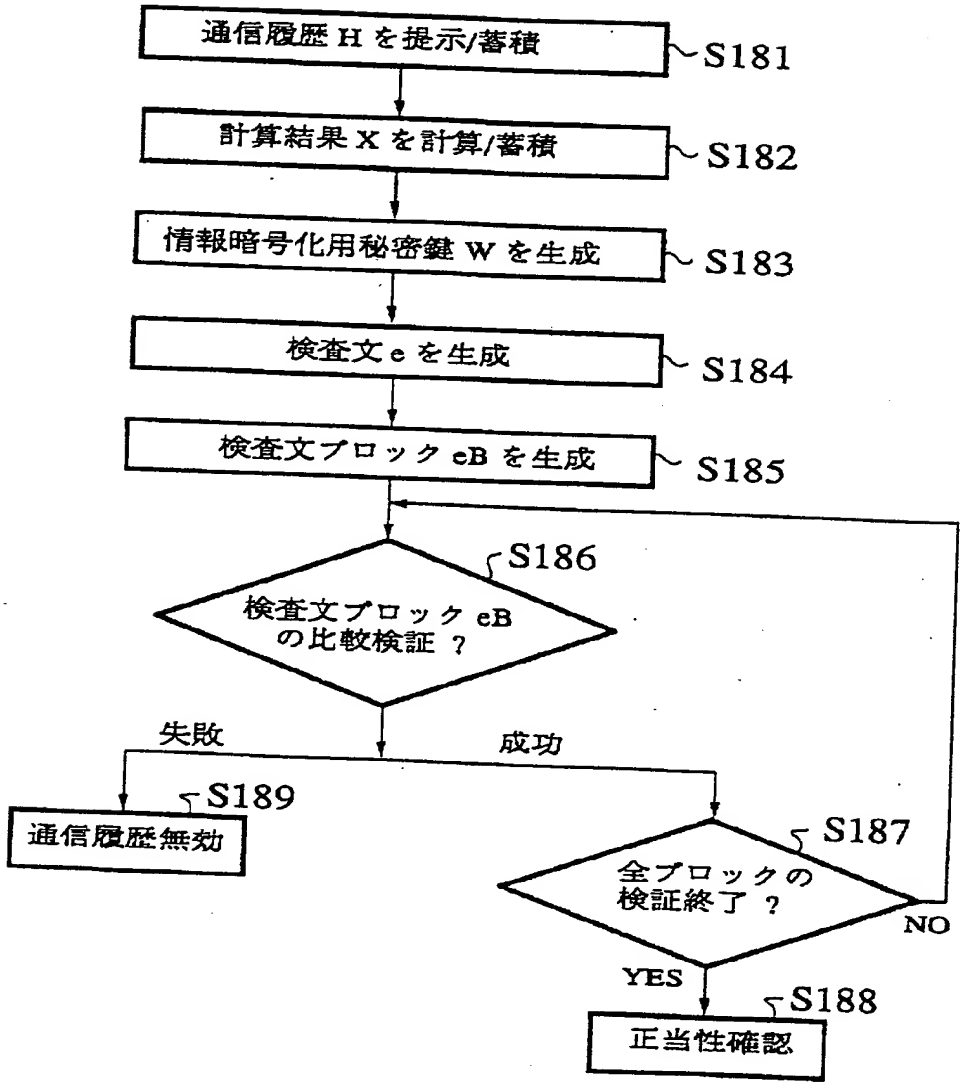
【図10】


10利用者(端末)
20情報提供者(端末)
30通信回線
40調停者(端末)
100
101 利用者秘密情報蓄積手段
102 一時メモリ
103 乱数発生手段
104 演算手段
105 共通鍵暗号手段
106 情報出力/利用手段
107 公開鍵暗号手段
108 情報再構成手段
109 情報蓄積手段
200 通信制御手段
201 情報提供者秘密情報蓄積手段
202 情報データベース
203 一時メモリ
204 演算手段
205 共通鍵暗号手段
206 検証手段
207 情報分割手段
208 通信履歴ファイル
209 乱数発生手段
210 公開鍵暗号手段
401 演算手段
402 一時メモリ
403 検証手段
404 情報分割手段
405 公開鍵暗号手段

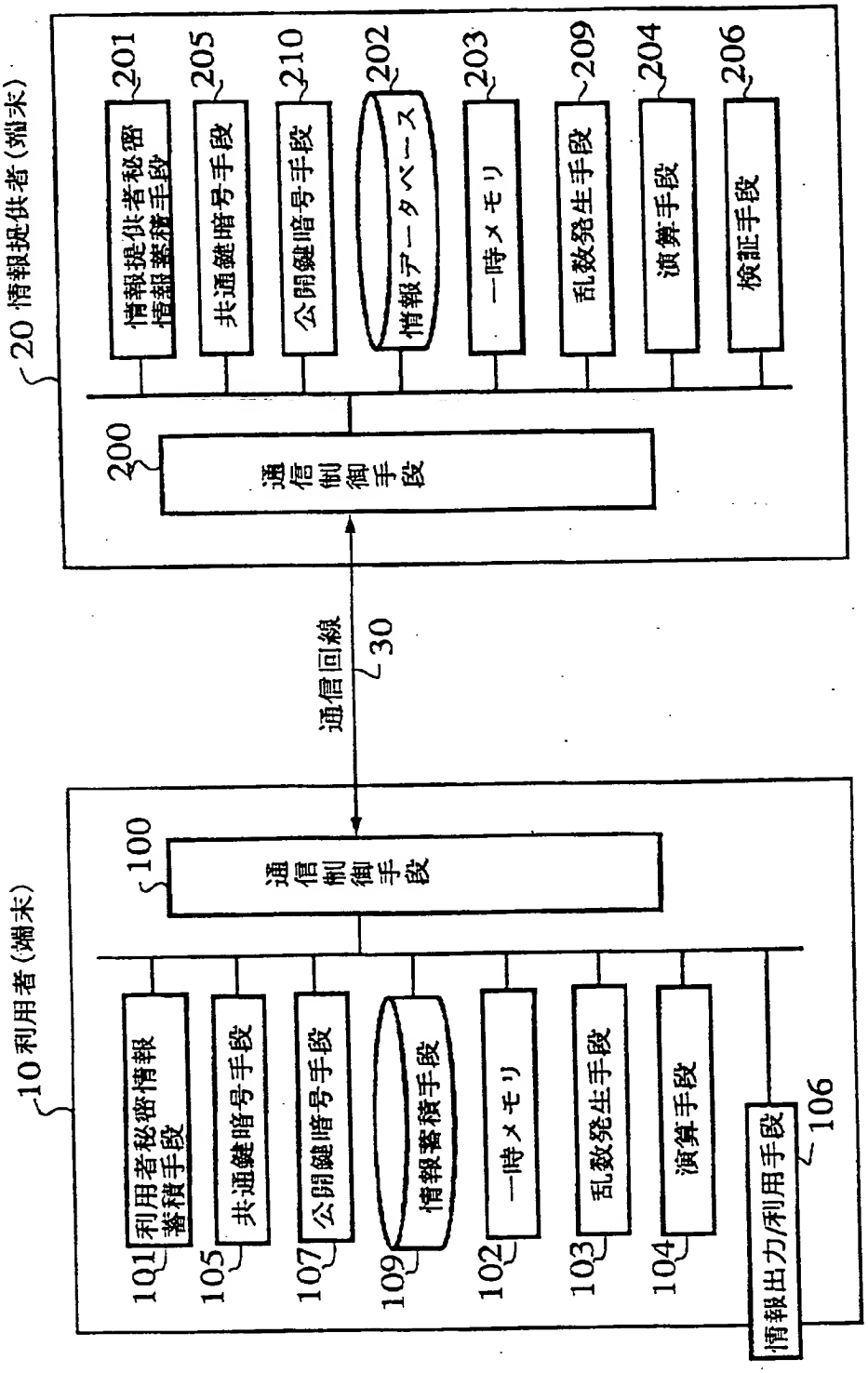
【図11】


S151
乱数Rの生成/蓄積
S152
初期応答文Xの計算
S153
初期応答文Xの送信
S154
初期応答文Xの受信/蓄積
S155
乱数文Zの生成/蓄積
S156
情報暗号化用秘密鍵Wの生成/蓄積
S157
情報Mの取り出し
S158
情報Mの暗号化,暗号文Cの送信
S159
暗号文Cの受信/蓄積,受信通知
S160
検査文eの作成/蓄積
S161
検査文ブロックeBの生成/蓄積
S162
検査文ブロックeBの送信
S163
検査文ブロックeBの受信/蓄積
S164
応答文Yの計算
S165
応答文Yの送信
S166
応答文Yの受信/蓄積
S167
検証 $Y^2=X\times I^e \pmod{N1}$?
成功
失敗
S168
プロトコル中止
S169
全ブロックの配送終了?
NO
YES
S170
通信履歴Hの記録管理
S171
検査文eの再構成
S172
情報暗号化用秘密鍵Wの獲得/蓄積
S173
暗号文Cの復号,情報Mの取り出し

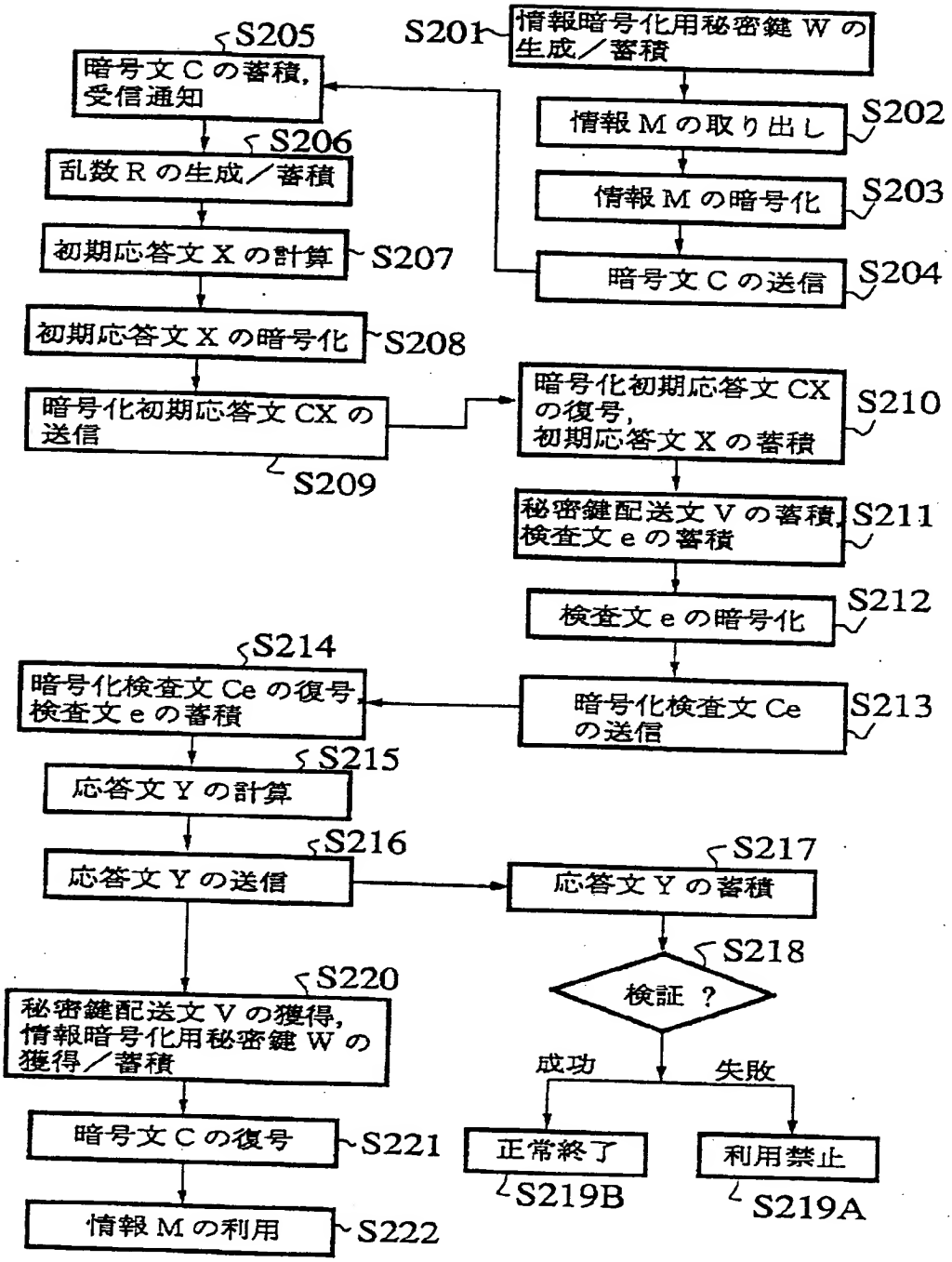
【図１２】


通信履歴Ｈを提示/蓄積
S181
計算結果Ｘを計算/蓄積
S182
情報暗号化用秘密鍵Ｗを生成
S183
検査文ｅを生成
S184
検査文ブロックｅＢを生成
S185
S186
検査文ブロックｅＢの比較検証？
失敗
成功
S189
通信履歴無効
S187
全ブロックの検証終了？
NO
YES
S188
正当性確認

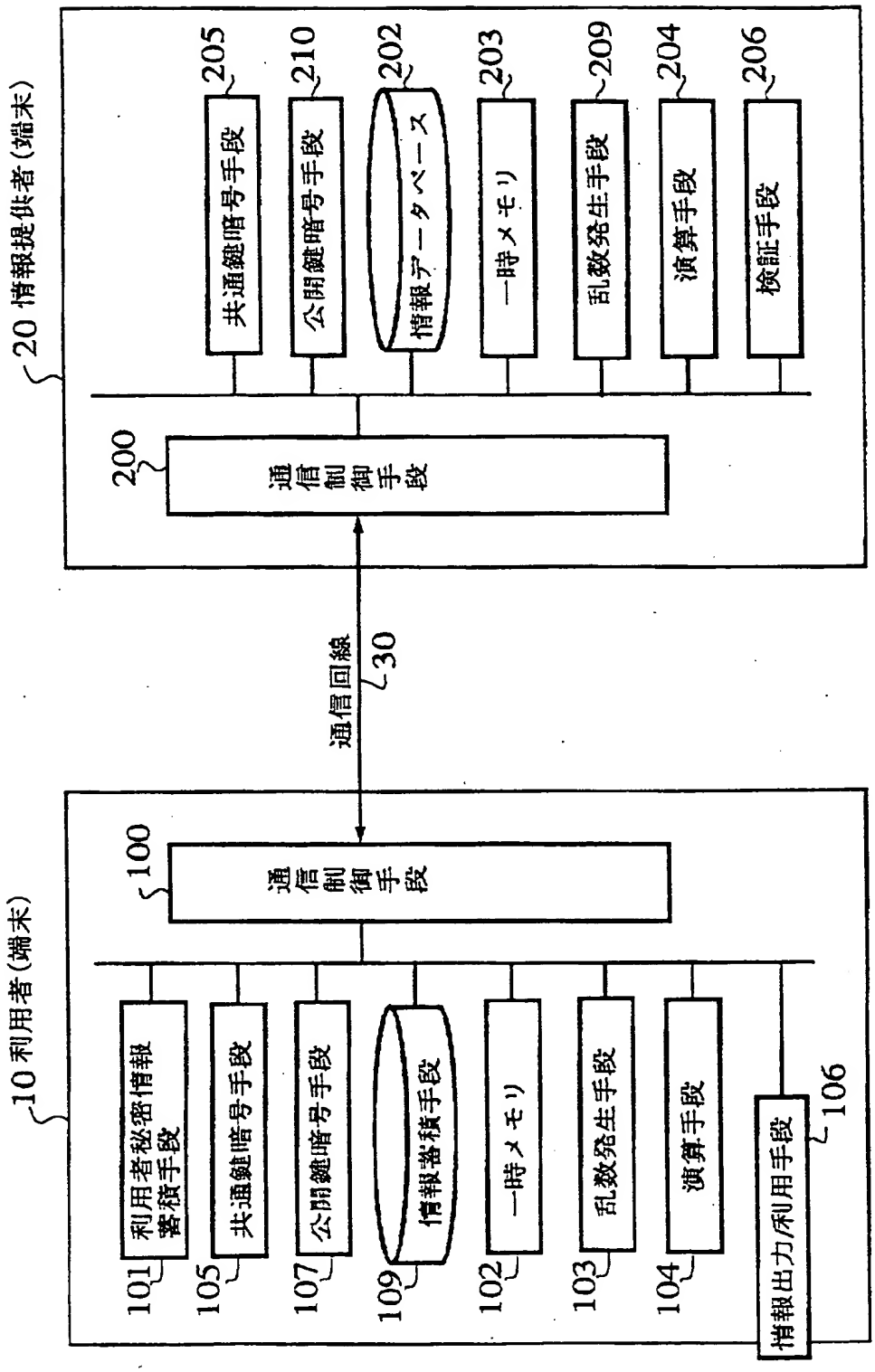
【図13】


10 利用者(端末)
20 情報提供者(端末)
30
通信回線
100
通信制御手段
101
利用者秘密情報蓄積手段
105
共通鍵暗号手段
107
公開鍵暗号手段
109
情報蓄積手段
102
一時メモリ
103
乱数発生手段
104
演算手段
106
情報出力/利用手段
200
通信制御手段
201
情報提供者秘密情報蓄積手段
205
共通鍵暗号手段
210
公開鍵暗号手段
202
情報データベース
203
一時メモリ
209
乱数発生手段
204
演算手段
206
検証手段

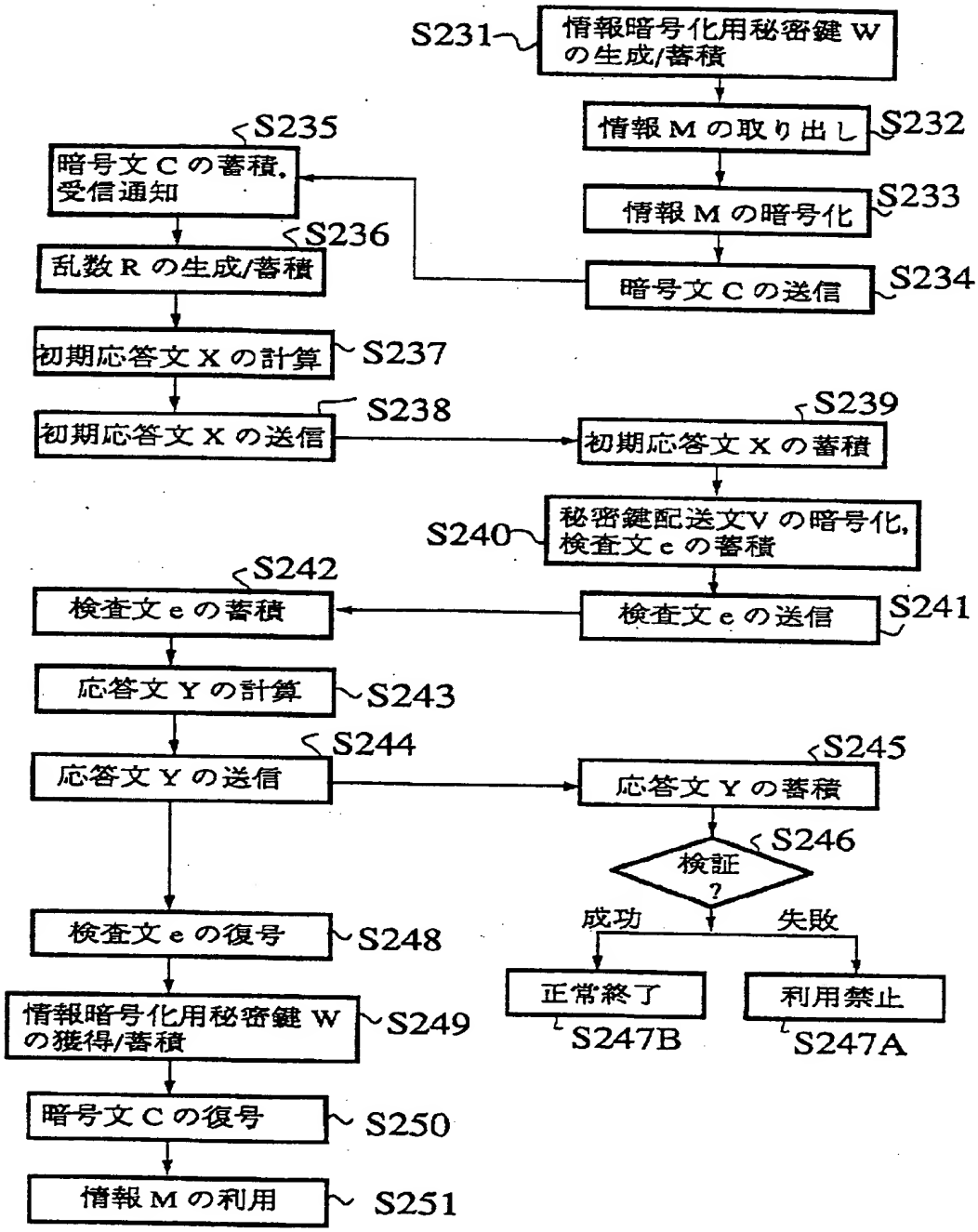
【図14】


S201
情報暗号化用秘密鍵Wの生成／蓄積
S202
情報Mの取り出し
S203
情報Mの暗号化
S204
暗号文Cの送信
S205
暗号文Cの蓄積，受信通知
S206
乱数Rの生成／蓄積
S207
初期応答文Xの計算
S208
初期応答文Xの暗号化
S209
暗号化初期応答文CXの送信
S210
暗号化初期応答文CXの復号，初期応答文Xの蓄積
S211
秘密鍵配送文Vの蓄積，検査文eの蓄積
S212
検査文eの暗号化
S213
暗号化検査文Ceの送信
S214
暗号化検査文Ceの復号，検査文eの蓄積
S215
応答文Yの計算
S216
応答文Yの送信
S217
応答文Yの蓄積
S218
検証？
成功
失敗
S219A
利用禁止
S219B
正常終了
S220
秘密鍵配送文Vの獲得，情報暗号化用秘密鍵Wの獲得／蓄積
S221
暗号文Cの復号
S222
情報Mの利用

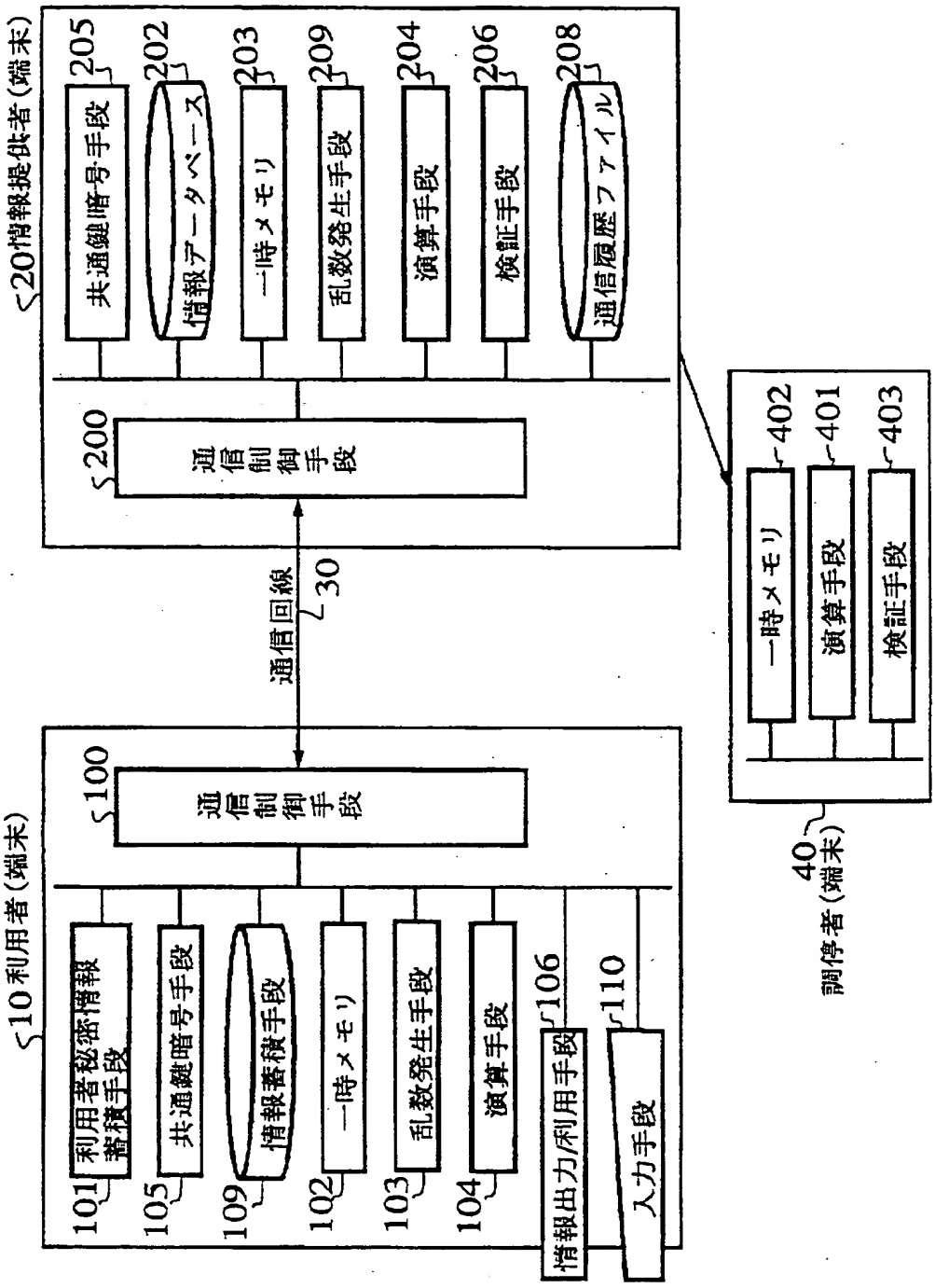
【図15】


20 情報提供者(端末)
205
共通鍵暗号手段
210
公開鍵暗号手段
202
情報データベース
203
一時メモリ
209
乱数発生手段
204
演算手段
206
検証手段
200
通信制御手段
通信回線
30
10 利用者(端末)
100
通信制御手段
101
利用者秘密情報蓄積手段
105
共通鍵暗号手段
107
公開鍵暗号手段
109
情報蓄積手段
102
一時メモリ
103
乱数発生手段
104
演算手段
106
情報出力/利用手段

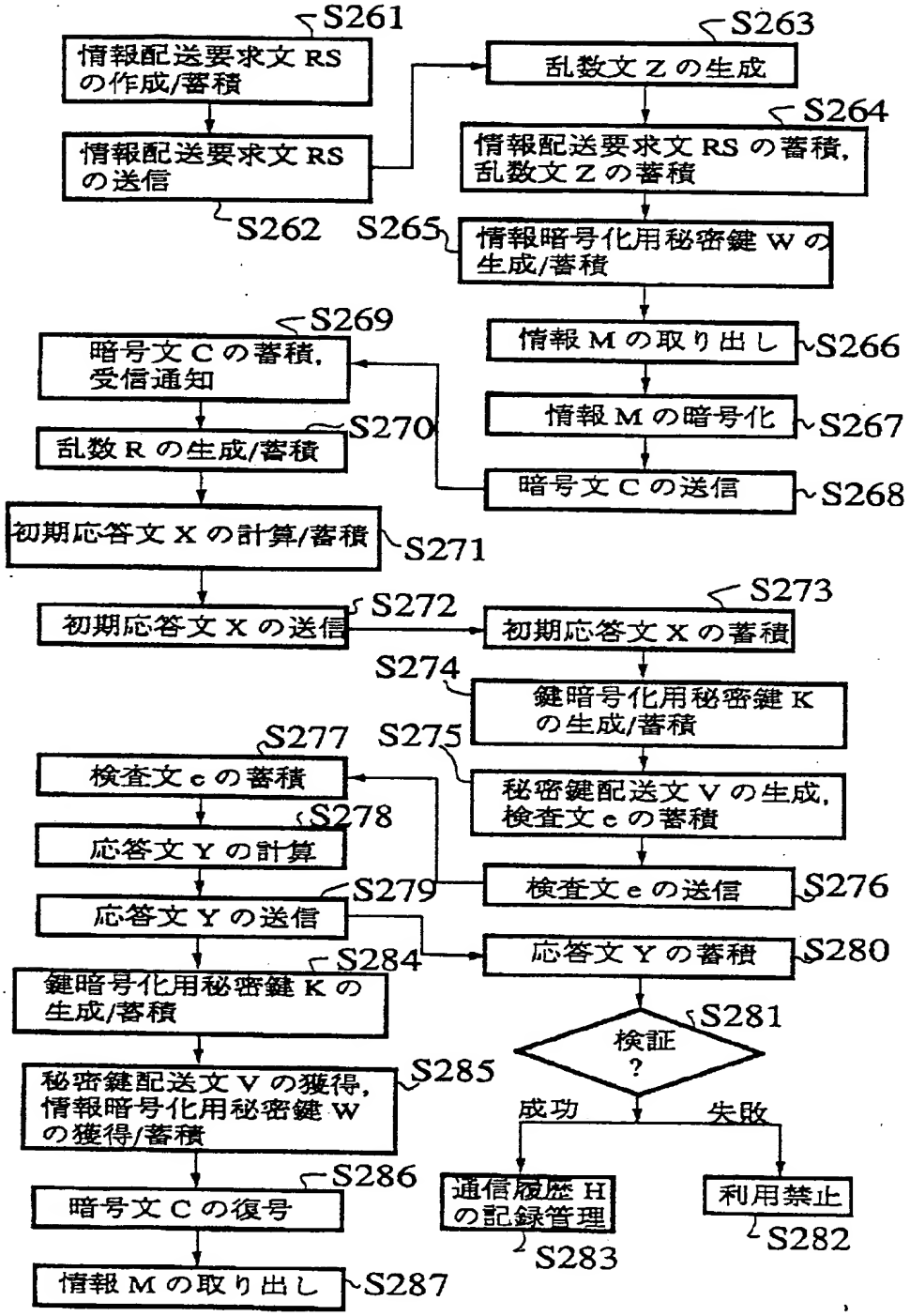
【図16】


S231
情報暗号化用秘密鍵Wの生成/蓄積
情報Mの取り出し
S232
情報Mの暗号化
S233
暗号文Cの送信
S234
S235
暗号文Cの蓄積,受信通知
S236
乱数Rの生成/蓄積
初期応答文Xの計算
S237
初期応答文Xの送信
S238
S239
初期応答文Xの蓄積
S240
秘密鍵配送文Vの暗号化,検査文eの蓄積
検査文eの送信
S241
S242
検査文eの蓄積
応答文Yの計算
S243
応答文Yの送信
S244
S245
応答文Yの蓄積
S246
検証?
成功
失敗
正常終了
S247B
利用禁止
S247A
検査文eの復号
S248
情報暗号化用秘密鍵Wの獲得/蓄積
S249
暗号文Cの復号
S250
情報Mの利用
S251

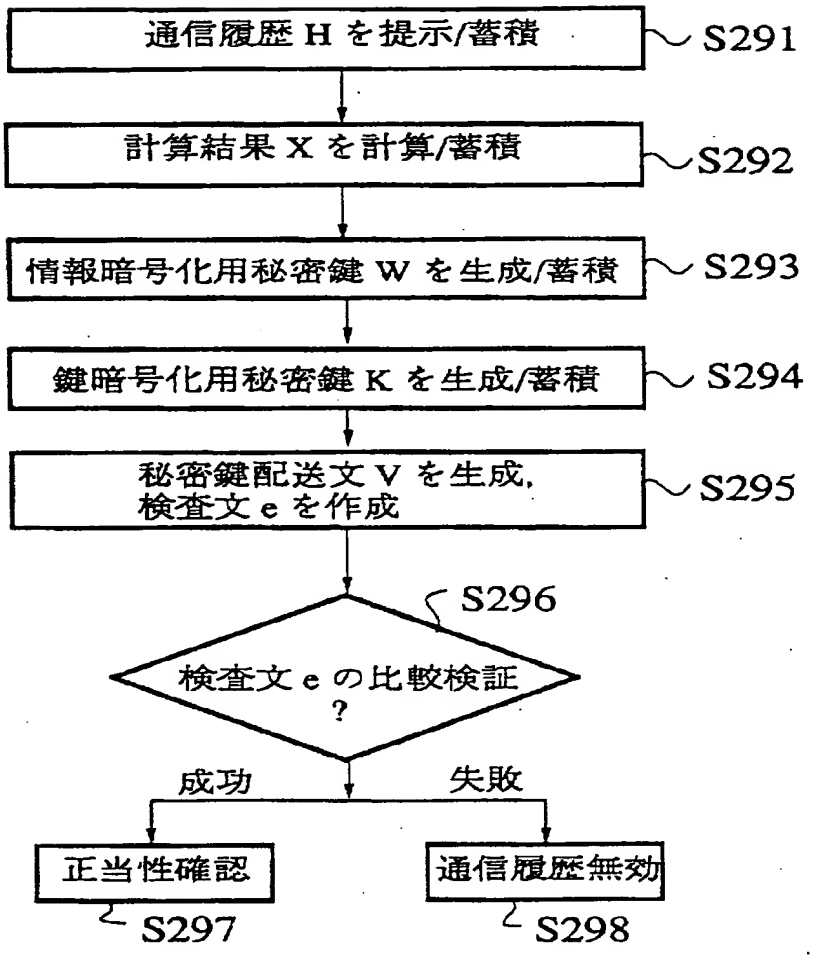
【図１７】


20 情報提供者（端末）
205 共通鍵暗号手段
202 情報データベース
203 一時メモリ
209 乱数発生手段
204 演算手段
206 検証手段
208 通信履歴ファイル
200 通信制御手段
通信回線 30
10 利用者（端末）
100 通信制御手段
101 利用者秘密情報蓄積手段
105 共通鍵暗号手段
109 情報蓄積手段
102 一時メモリ
103 乱数発生手段
104 演算手段
106 情報出力/利用手段
110 入力手段
40 調停者（端末）
402 一時メモリ
401 演算手段
403 検証手段

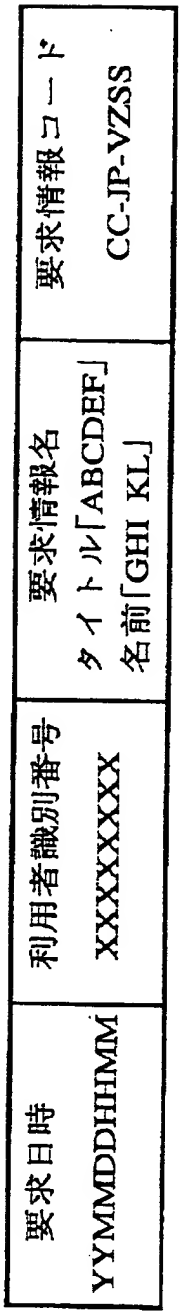
【図１８】


S261
情報配送要求文 RS の作成/蓄積
情報配送要求文 RS の送信
S262
S263
乱数文 Z の生成
S264
情報配送要求文 RS の蓄積，乱数文 Z の蓄積
S265
情報暗号化用秘密鍵 W の生成/蓄積
S266
情報 M の取り出し
S267
情報 M の暗号化
S268
暗号文 C の送信
S269
暗号文 C の蓄積，受信通知
S270
乱数 R の生成/蓄積
S271
初期応答文 X の計算/蓄積
S272
初期応答文 X の送信
S273
初期応答文 X の蓄積
S274
鍵暗号化用秘密鍵 K の生成/蓄積
S275
秘密鍵配送文 V の生成，検査文 e の蓄積
S276
検査文 e の送信
S277
検査文 e の蓄積
S278
応答文 Y の計算
S279
応答文 Y の送信
S280
応答文 Y の蓄積
S281
検証 ?
成功
失敗
S282
利用禁止
S283
通信履歴 H の記録管理
S284
鍵暗号化用秘密鍵 K の生成/蓄積
S285
秘密鍵配送文 V の獲得，情報暗号化用秘密鍵 W の獲得/蓄積
S286
暗号文 C の復号
S287
情報 M の取り出し

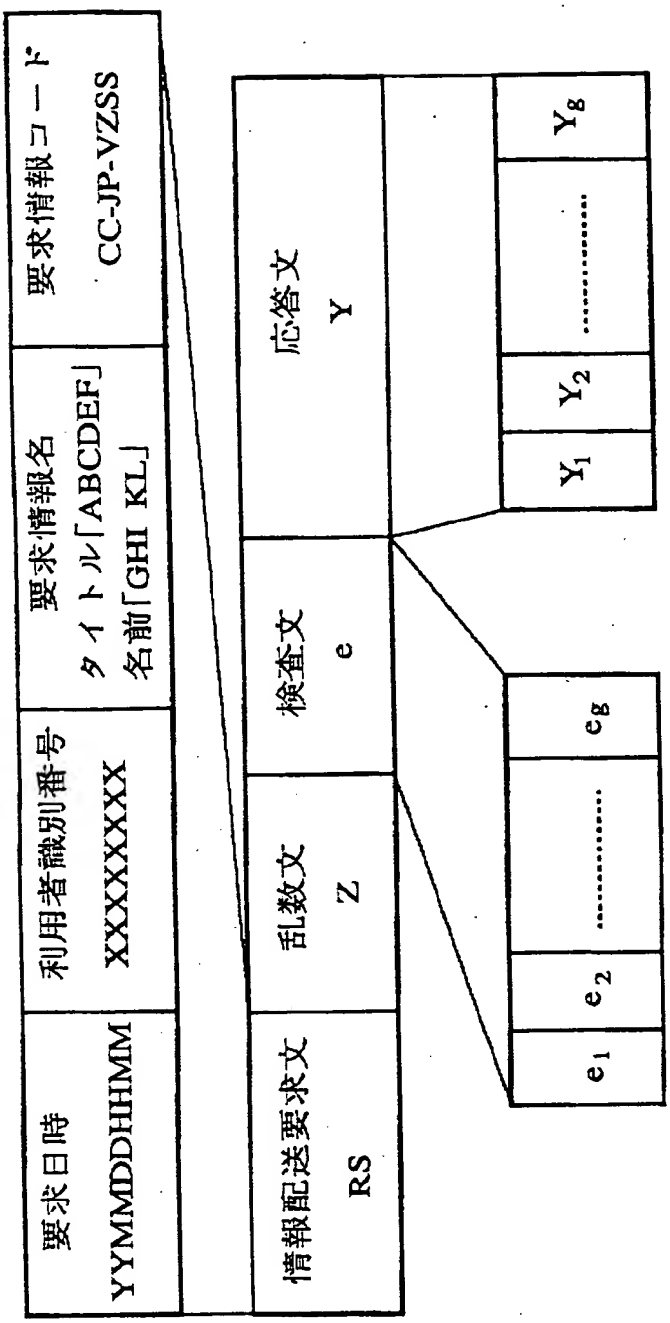
【図１９】


通信履歴Ｈを提示/蓄積
S291
計算結果Ｘを計算/蓄積
S292
情報暗号化用秘密鍵Ｗを生成/蓄積
S293
鍵暗号化用秘密鍵Ｋを生成/蓄積
S294
秘密鍵配送文Ｖを生成,
検査文ｅを作成
S295
S296
検査文ｅの比較検証
?
成功
失敗
正当性確認
S297
通信履歴無効
S298

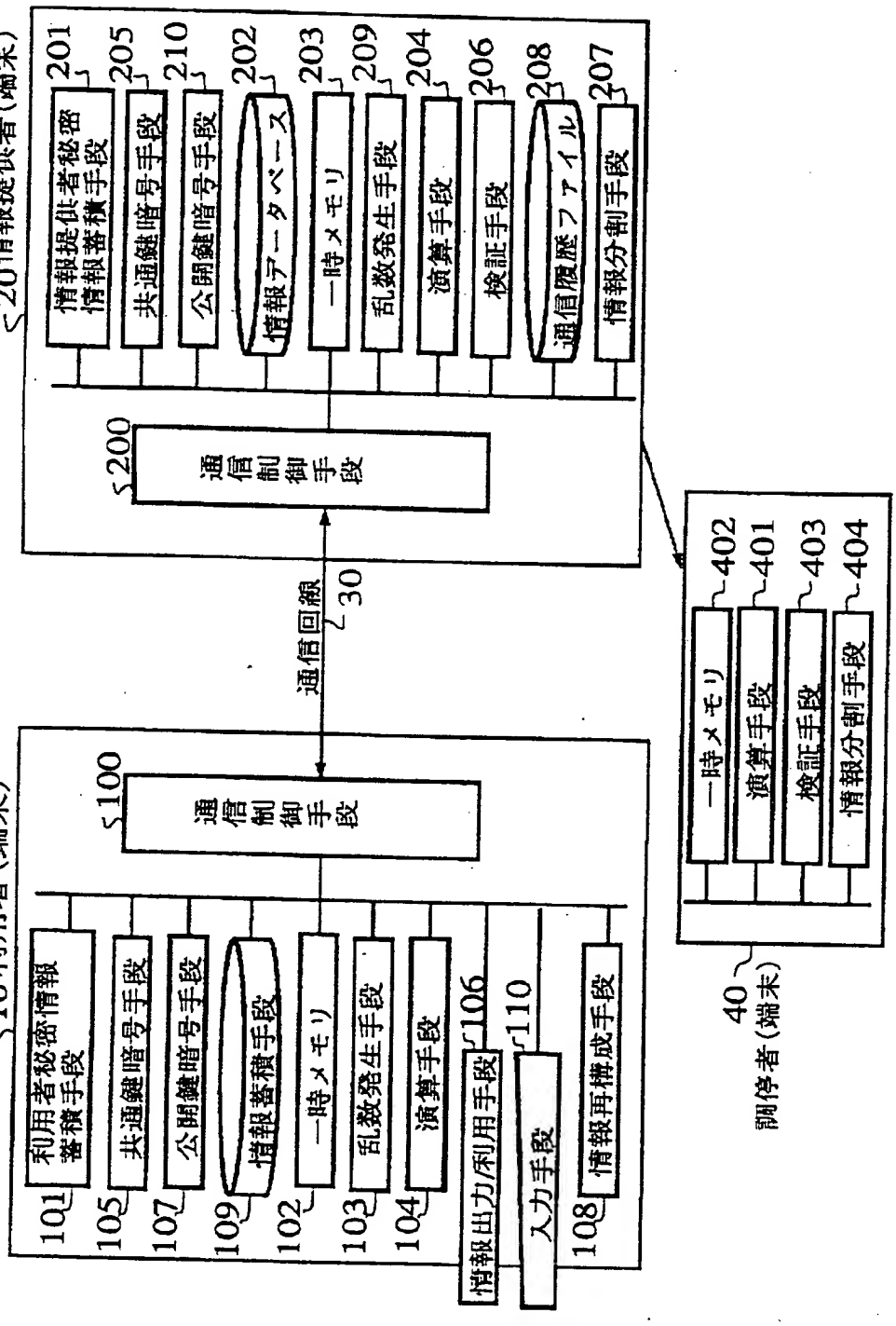
【図２０】


要求日時
YYMMDDHHMM
利用者識別番号
XXXXXXXXX
要求情報名
タイトル「ABCDEF」
名前「GHI KL」
要求情報コード
CC-JP-VZSS

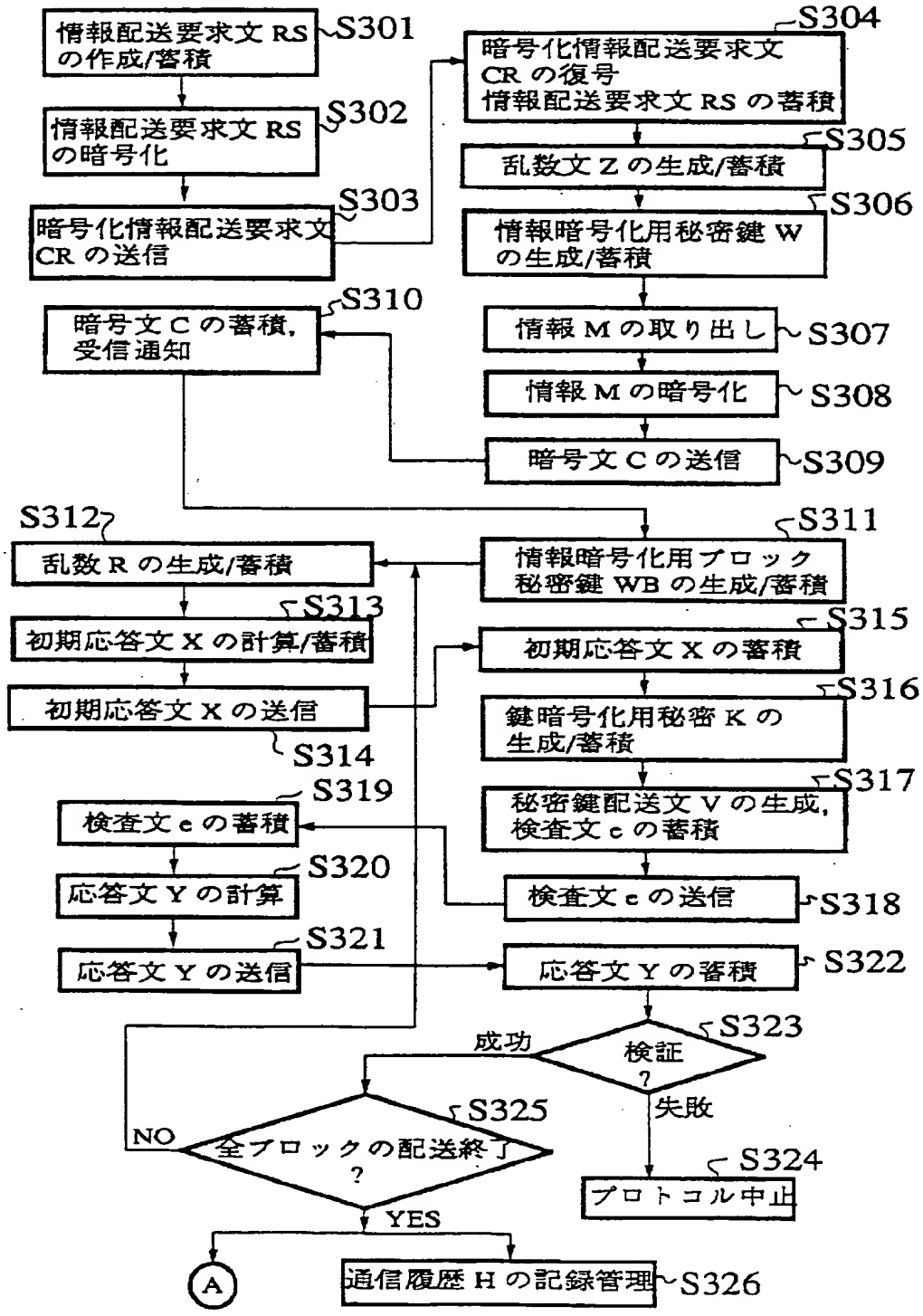
【図21】


要求日時
YYMMDDHHMM
利用者識別番号
XXXXXXXXX
要求情報名
タイトル「ABCDEF」
名前「GHI KL」
要求情報コード
CC-JP-VZSS
情報配送要求文
RS
乱数文
Z
検査文
e
応答文
Y
e1
e2
.....
eg
Y1
Y2
.....
Yg

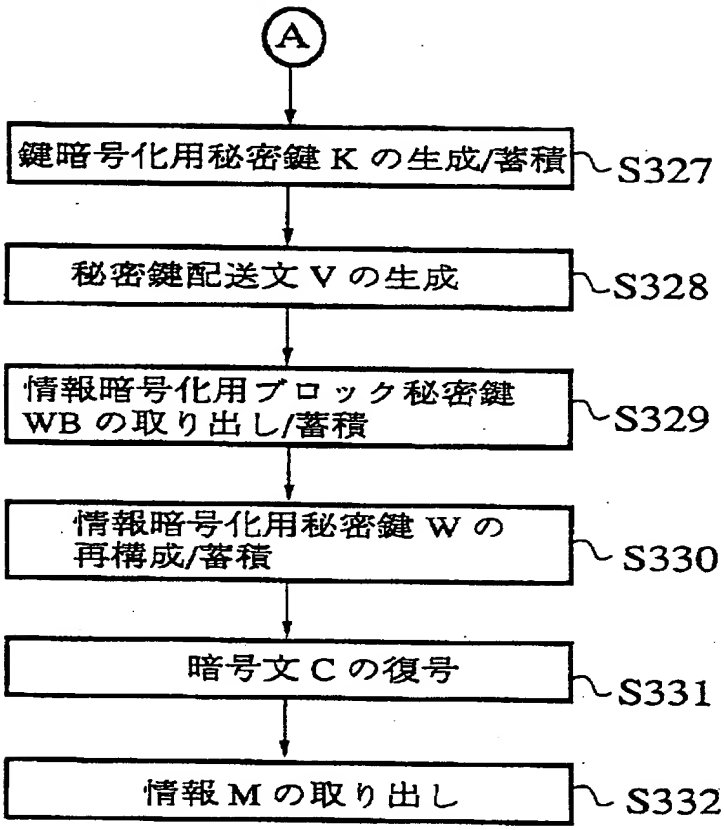
【図22】


10利用者(端末)
20情報提供者(端末)
30通信回線
40課停者(端末)
100通信制御手段
101利用者秘密情報蓄積手段
102情報蓄積手段
103一時メモリ
104乱数発生手段
105共通鍵暗号手段
106情報出力/利用手段
107公開鍵暗号手段
108情報再構成手段
109演算手段
110入力手段
200通信制御手段
201情報提供者秘密情報蓄積手段
202情報データベース
203一時メモリ
204乱数発生手段
205共通鍵暗号手段
206検証手段
207情報分割手段
208通信履歴ファイル
209演算手段
210公開鍵暗号手段
401演算手段
402一時メモリ
403検証手段
404情報分割手段

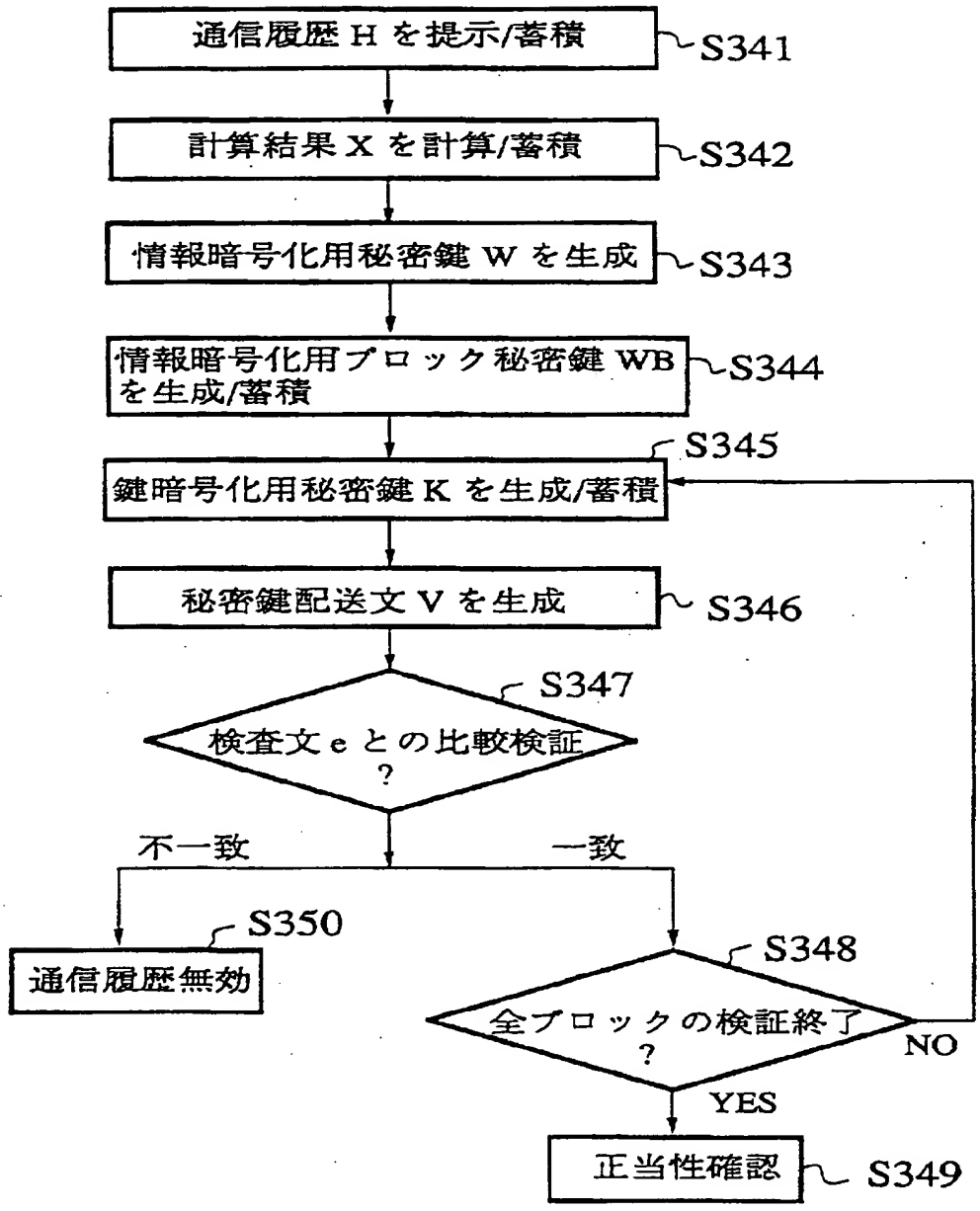
【図２３】


情報配送要求文 RS の作成/蓄積
S301
情報配送要求文 RS の暗号化
S302
暗号化情報配送要求文 CR の送信
S303
暗号化情報配送要求文 CR の復号 情報配送要求文 RS の蓄積
S304
乱数文 Z の生成/蓄積
S305
情報暗号化用秘密鍵 W の生成/蓄積
S306
情報 M の取り出し
S307
情報 M の暗号化
S308
暗号文 C の送信
S309
暗号文 C の蓄積, 受信通知
S310
情報暗号化用ブロック秘密鍵 WB の生成/蓄積
S311
乱数 R の生成/蓄積
S312
初期応答文 X の計算/蓄積
S313
初期応答文 X の送信
S314
初期応答文 X の蓄積
S315
鍵暗号化用秘密 K の生成/蓄積
S316
秘密鍵配送文 V の生成, 検査文 c の蓄積
S317
検査文 c の送信
S318
検査文 e の蓄積
S319
応答文 Y の計算
S320
応答文 Y の送信
S321
応答文 Y の蓄積
S322
検証 ?
S323
成功
失敗
全ブロックの配送終了 ?
S325
NO
YES
プロトコル中止
S324
通信履歴 H の記録管理
S326
A

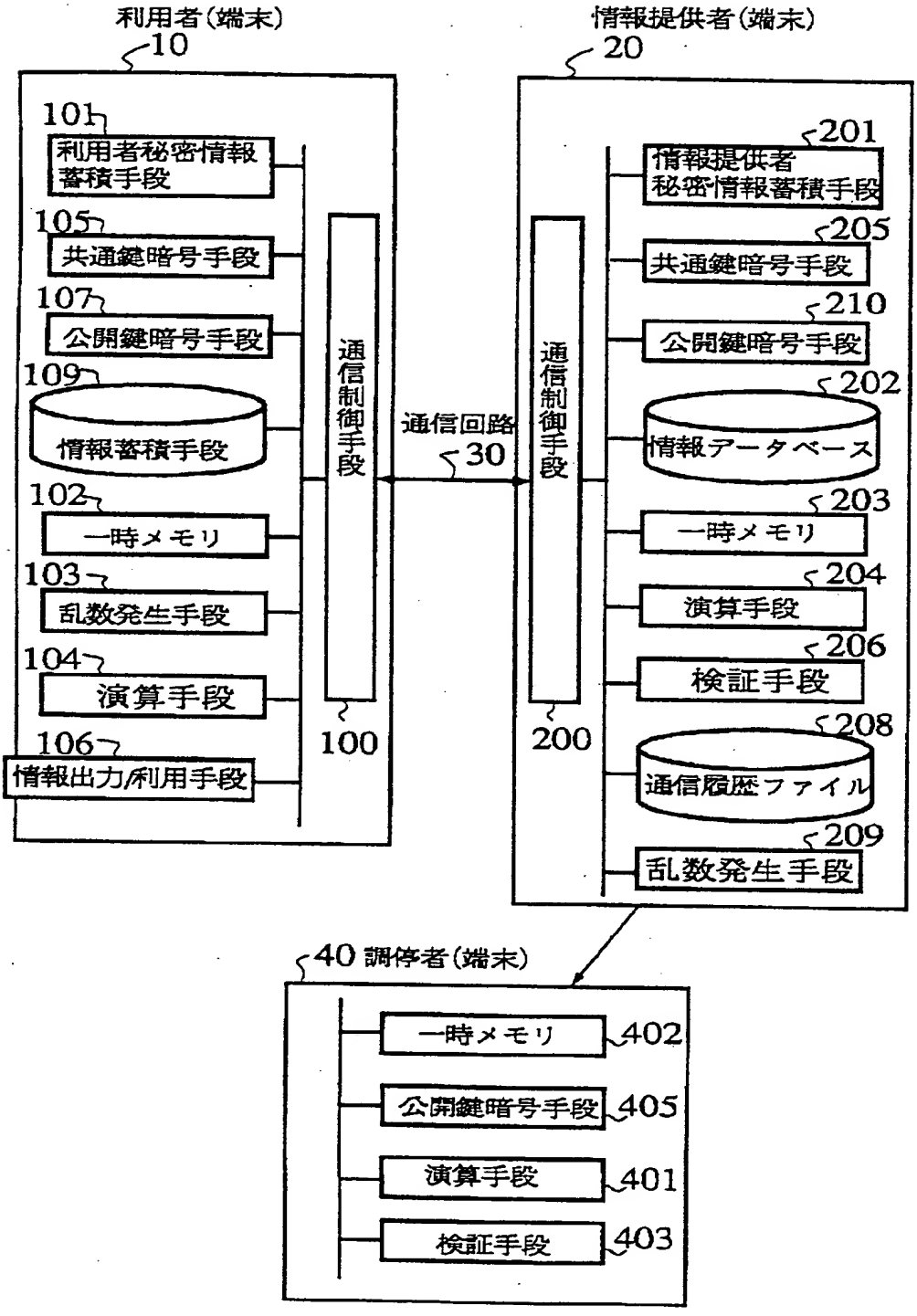
【図２４】


A
鍵暗号化用秘密鍵Ｋの生成/蓄積
S327
秘密鍵配送文Ｖの生成
S328
情報暗号化用ブロック秘密鍵
WBの取り出し/蓄積
S329
情報暗号化用秘密鍵Ｗの
再構成/蓄積
S330
暗号文Ｃの復号
S331
情報Ｍの取り出し
S332

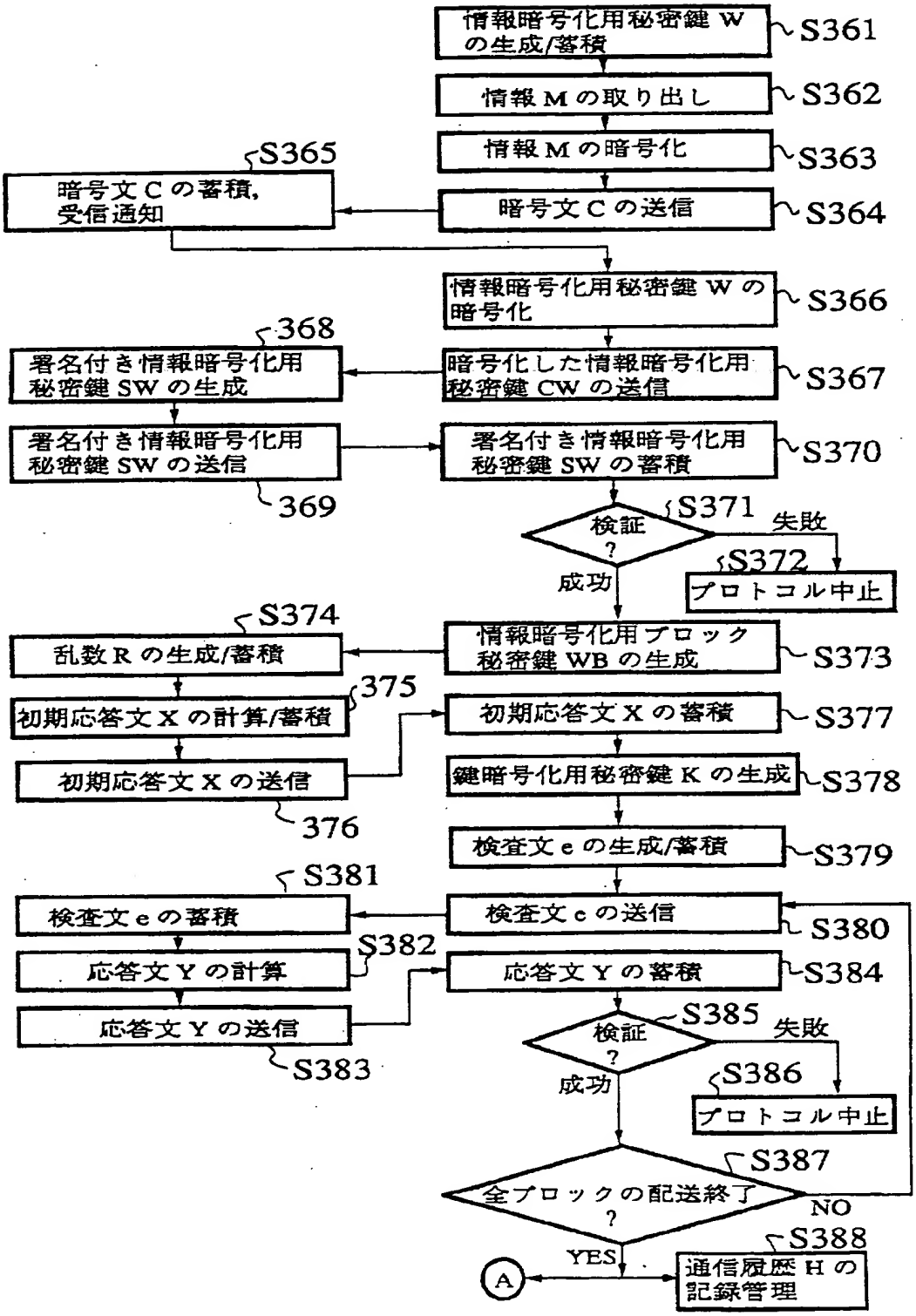
【図２５】


通信履歴Ｈを提示/蓄積
S341
計算結果Ｘを計算/蓄積
S342
情報暗号化用秘密鍵Ｗを生成
S343
情報暗号化用ブロック秘密鍵WBを生成/蓄積
S344
S345
鍵暗号化用秘密鍵Ｋを生成/蓄積
秘密鍵配送文Ｖを生成
S346
S347
検査文ｅとの比較検証?
不一致
一致
S350
通信履歴無効
S348
全ブロックの検証終了?
NO
YES
正当性確認
S349

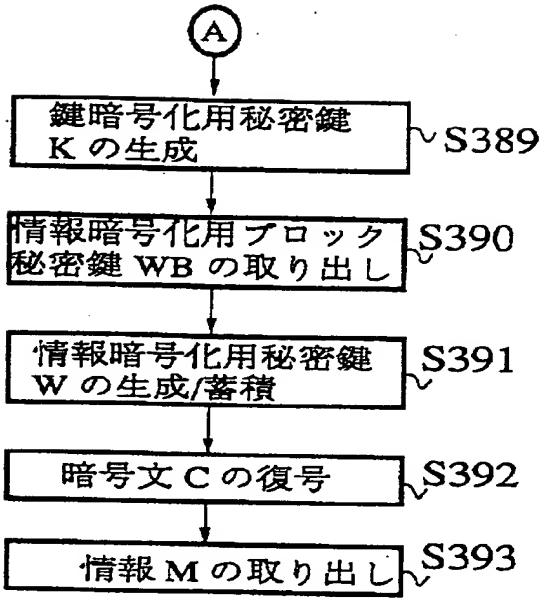
【図２６】


利用者(端末)
10
101
利用者秘密情報蓄積手段
105
共通鍵暗号手段
107
公開鍵暗号手段
109
情報蓄積手段
102
一時メモリ
103
乱数発生手段
104
演算手段
106
情報出力/利用手段
通信制御手段
100
通信回路
30
情報提供者(端末)
20
通信制御手段
200
201
情報提供者秘密情報蓄積手段
205
共通鍵暗号手段
210
公開鍵暗号手段
202
情報データベース
203
一時メモリ
204
演算手段
206
検証手段
208
通信履歴ファイル
209
乱数発生手段
40 調停者(端末)
一時メモリ
402
公開鍵暗号手段
405
演算手段
401
検証手段
403

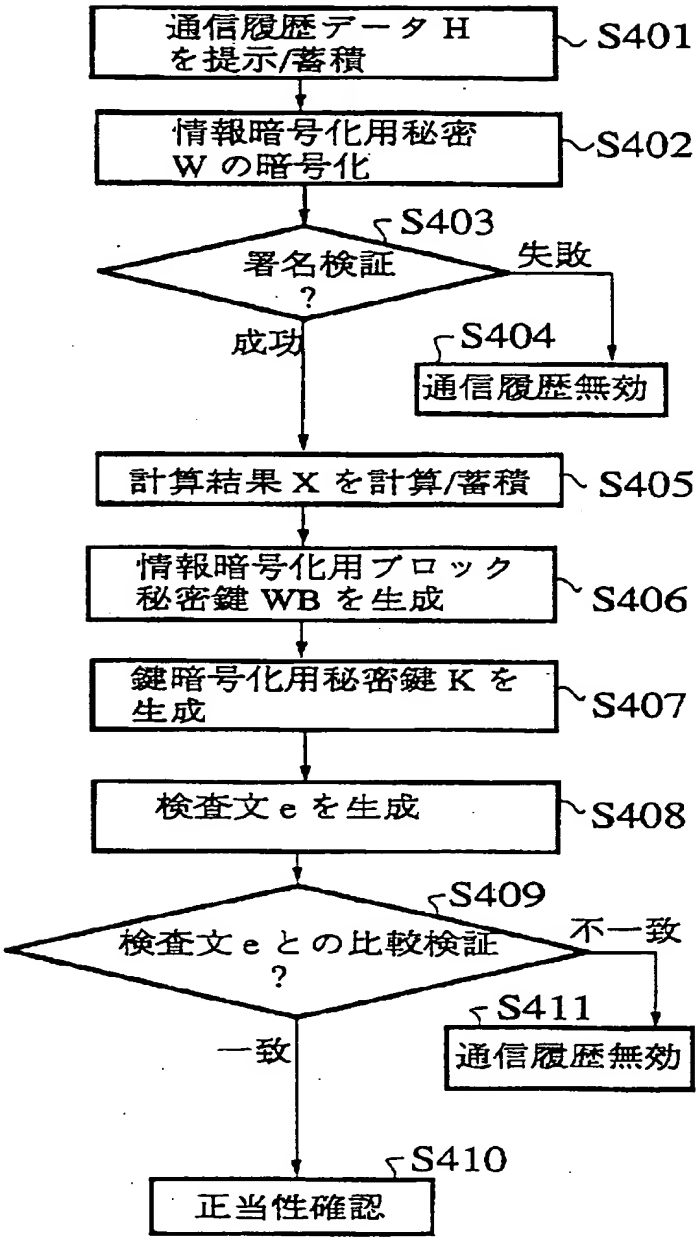
【図２７】


情報暗号化用秘密鍵Wの生成/蓄積
S361
情報Mの取り出し
S362
情報Mの暗号化
S363
暗号文Cの送信
S364
S365
暗号文Cの蓄積,受信通知
情報暗号化用秘密鍵Wの暗号化
S366
暗号化した情報暗号化用秘密鍵CWの送信
S367
368
署名付き情報暗号化用秘密鍵SWの生成
署名付き情報暗号化用秘密鍵SWの送信
369
署名付き情報暗号化用秘密鍵SWの蓄積
S370
検証?
S371
失敗
S372
プロトコル中止
成功
情報暗号化用ブロック秘密鍵WBの生成
S373
S374
乱数Rの生成/蓄積
375
初期応答文Xの計算/蓄積
初期応答文Xの送信
376
初期応答文Xの蓄積
S377
鍵暗号化用秘密鍵Kの生成
S378
検査文eの生成/蓄積
S379
S381
検査文eの蓄積
検査文cの送信
S380
S382
応答文Yの計算
応答文Yの送信
S383
応答文Yの蓄積
S384
検証?
S385
失敗
S386
プロトコル中止
成功
全ブロックの配送終了?
S387
NO
YES
S388
通信履歴Hの記録管理
A

【図２８】


A
鍵暗号化用秘密鍵Kの生成
S389
情報暗号化用ブロック秘密鍵WBの取り出し
S390
情報暗号化用秘密鍵Wの生成/蓄積
S391
暗号文Cの復号
S392
情報Mの取り出し
S393

【図２９】



フロントページの続き

(51)Int.Cl.⁶	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０９Ｃ　1/00		7259－5Ｊ		